Plan de gestión mediante la guía del PMBOK para la planificación estratégica del sistema de gestión de la seguridad informática (SGSI) NTC ISO 27001:2013 para la Clínica Medical Duarte

Victor Manuel Garnica Carrillo

Universidad Nacional Abierta y a Distancia
Escuela de Ciencias Básicas, Tecnología e Ingeniería (ECBTI)
Especialización en Seguridad Informática
Cúcuta
2018

Plan de gestión mediante la guía del PMBOK para la planificación estratégica del sistema de gestión de la seguridad informática (SGSI) NTC ISO 27001:2013 para la Clínica Medical Duarte

Victor Manuel Garnica Carrillo

Trabajo de Grado presentado como requisito para optar al título de:
Especialista en Seguridad Informática

Director:
Ingeniero Martin Cancelado

Universidad Nacional Abierta y a Distancia
Escuela de Ciencias Básicas, Tecnología e Ingeniería (ECBTI)
Especialización en Seguridad Informática
Cúcuta
2018

Nota de Aceptación

_____

_____

_____

_____

_____

Firma presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Cúcuta, Norte de Santander, 01 de octubre de 2020.

Dedicatoria

A mi Esposa e Hija,

A mis padres

La preocupación por el hombre y su destino siempre debe ser el interés primordial de todo esfuerzo técnico. Nunca olvides esto entre tus diagramas y ecuaciones.

Albert Einstein

Agradecimientos

A dios por la fortaleza concebida para lograr los objetivos de culminar el presente proyecto.

A la Clínica médica duarte y directivos por la oportunidad otorgada para la realización de la Especialización en Seguridad Informática.

A mi esposa e hija por su apoyo, comprensión y amor que me regalan a diario.

Resumen

El presente documento tiene como finalidad presentar un plan estructurado basado en la Guía PMBOK con respecto a los grupos de proceso de inicio y planificación para lograr el alcance y objetivos de realizar los procesos involucrados en dichos grupos con el fin de trazar los lineamientos para la planificación de la norma NTC ISO 27001:2013. El desarrollo del proyecto incluyo en explorar la institución de estudio y sus objetivos principales, a partir de ello se inicia la construcción y recopilación para el alcance del proyecto relacionado con los grupos de procesos del PMBOK. El plan de dirección de proyecto mediante un formato diseñado mediante las mejores prácticas de la guía del PMBOK mediante una serie de documento que nos permitirán dirigir la ejecución, monitoreo, control y cierre. Este nos permite recopilar los requisitos del proyecto y producto, las líneas base del alcance, cronograma y costo, como también se estipula los planes requeridos por el alcance del proyecto. Es importante diseñar la EDT o la Estructura Detalla de Trabajo, que suministrara pautas para organizar las actividades en la planificación del trabajo según la norma NTC ISO 27001:2013 a utilizar. Se ha definido mediante la ayuda del PMBOK la relación de los interesados con el plan del proyecto que permitirán definir aquellos actores que afectarán positiva o negativamente el mismo. Se considera que el existo de esta norma, es realizar un estudio profundo para interpretarla y generar las estrategias que requiere el trabajo. Debido al alcance del proyecto se recomienda complementar en una segunda etapa, los demás grupos de procesos que posee el PMBOK, como beneficio del proyecto en general.

Palabras clave: guía PMBOK, NTC ISO 27001:2013, grupos, normas, procesos, PMI.

Abstract

The purpose of this document is to present a structured plan based on the PMBOK Guide regarding the initiation and planning process groups to achieve the scope and objectives of carrying out the processes involved in said groups in order to draw the guidelines for planning. of the NTC ISO 27001: 2013 standard. The development of the project includes exploring the institution of study and its main objectives, from which the construction and compilation for the scope of the project related to the PMBOK process groups begins. The project management plan through a format designed using the best practices of the PMBOK guide through a series of documents that will allow us to direct the execution, monitoring, control and closure. This allows us to compile the requirements of the project and product, the baselines of the scope, schedule and cost, as well as the plans required by the scope of the project. It is important to design the EDT or the Detailed Work Structure, which will provide guidelines to organize the activities in the work planning according to the NTC ISO 27001: 2013 standard to be used. Through the help of the PMBOK, the relationship of the stakeholders with the project plan has been defined, which will allow defining those actors that will positively or negatively affect it. It is considered that the existence of this norm is to carry out an in-depth study to interpret it and generate the strategies that the work requires. Due to the scope of the project, it is recommended to complement in a second stage, the other groups of processes that have the PMBOK, as a benefit of the project in general.

Keywords: PMBOK guide, NTC ISO 27001: 2013, groups, standards, processes, PM

Tabla de contenido

Contenido

Lista de figuras

Lista de tablas

Introducción

Las empresas no perciben el potencial daño que pueden generar hoy en día un ataque informático a raíz de brechas de seguridad, políticas insuficientes, campañas de control y capacitación que puedan mitigar riesgos y crear salvaguardas. La implementación de un Sistema de Gestión de la Seguridad Informática lograría fortalecer y abarcar muchos ámbitos de la institución, para ello este documento plantea la planificación utilizando como medio estratégico, la guía del PMBOK y sus mejores prácticas, estándares, pautas y normas para la planificación y dirección de proyectos, sobre la estructura necesaria y pasos que se requieren para lograr su implementación acorde a los planes de gestión que se estudien en el presente documento.

Recopilando las mejores prácticas del PMBOK, recopilaremos la información actual de la institución objeto de estudio, mediante la planificación y definición del acta de constitución del proyecto y definición de interesados de este. Un plan importante de las mejores prácticas del PMBOK, es definir el plan de dirección del proyecto, cuyo documento nos permite dirigir la ejecución, monitoreo, control durante la vida del proyecto y finalmente el cierre de este. Mediante el plan de dirección del proyecto, podremos recopilar los requisitos del proyecto y producto final, las líneas fundamentales para lograr el alcance definido, cronograma y costo para el proyecto. Para este proyecto, se abarcarán los planes de gestión del alcance, gestión de requisitos y gestión del cronograma según se establece en la guía PMBOK.

Al definir la estructura detallada de trabajo o EDT, podemos tener una mayor relación de las actividades y pautas para la organización en la planificación y estudio de la norma NTC ISO 27001: 2013 a utilizar. Es importante hacer énfasis en el estudio minucioso y detallado de esta norma, por ello se crea un plan de trabajo o EDT que nos permitirá organizar las actividades a seguir y lograr el éxito general del proyecto.

Planeación.

1.1 TITULO

Plan de gestión mediante la guía del PMBOK para la planificación estratégica del SGSI NTC ISO 27001:2013 para la Clínica Medical Duarte

1.2 PROBLEMA

1.2.1 Definición del Problema.

La Clínica Medical Duarte (CMD) en búsqueda de la acreditación en salud, cuenta con una serie de políticas basadas en el aprendizaje del día a día, ideas ofrecidas por casa matriz o experiencia de los colaboradores del departamento de sistemas en pro de la seguridad de la información y protección de las redes. Estas políticas en ocasiones han surgido como ideas rápidas y breves solo por fines específicos mas no para las instituciones en general.

Las instituciones de salud en general deben estar provistos de mecanismos de seguridad que imposibiliten la incorporación de modificaciones a la Historia clínica una vez se registren y guarden los datos[1]. Además, deben preservar la información digital mediante políticas, medidas y estándares necesarios para asegurar la conservación a largo plazo de los documentos y expedientes electrónicos de archivo de tal manera que facilite su consulta en el tiempo[2].

Desde luego el personal encargado de la Tecnología e información, han implementado controles y técnicas conocidas para conservar, preservar y proteger la fuente de información[3], pero debemos preguntarnos ¿Es suficiente estos controles y en especial se establece, implementa, opera, se realiza seguimiento, revisión, mantenimiento y mejora continua en los sistemas de

---

[1] Resolución número 1995 de 1999, para establecer normal para el manejo de la Historia Clínica. https://www.minsalud.gov.co/Normatividad_Nuevo/RESOLUCI%C3%93N%201995%20DE%201999.pdf
[2] Acuerdo 003 de 2015 Lineamientos generales gestión de documentos electrónicos mediante el uso de medios electrónicos http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=61731
[3] Norma Técnica NTC-ISO/IEC Colombiana 27001

gestión actuales?, ¿Realmente se cumple a cabalidad todas las políticas y se realizan controles a las mismas?

La institución implementa métodos de seguridad basado en el conocimiento empírico e investigativo y lo que dicta las circunstancias del día por parte de los funcionarios, llevándolo a prácticas de seguridad esporádica y temporal. El departamento de sistemas es consciente de esta situación y busca día a día como proteger su información y demás activos que lo componen. La institución no cuenta con un Sistema de Gestión de la Seguridad de la Información formal como un aspecto fundamental para brindar un plan de diseño, implementación y mantenimiento con procesos que permitan continuar gestionando de manera eficiente la información, permitiendo fortalecer y asegurar la integridad, confidencialidad y disponibilidad de los datos.

1.2.2 Formulación del Problema.

Se considera que lograr un SGSI lograría abarcar algunos estándares que son dictaminadas por la gerencia de la información que se relaciona en el documento de Acreditación de Salud, Para lograr esto, este proyecto pretende plasmar y planificar el diseño, las directrices y pasos a seguir mediante la utilización de la guía PMBOK que permitirá buscar lineamientos planificados para la posterior implementación futura del SGSI.

1.3 JUSTIFICACIÓN

La Clínica Medical Duarte es una institución prestadora de salud con alta sensibilidad en sus procesos y regulados por entidades departamentales y nacionales.

Dada la importancia de la información que posee la institución, se da la necesidad de mantenerse seguros y confiables con respecto a todos los activos que componen la institución. Actualmente la institución cuenta con tecnología, hardware y software que cubre y resguardan las redes, algunos procesos y conocimientos implementados, pero ciertamente todo el control adecuado y

necesario para tratar los problemas de seguridad regulares como se ha presentado en varias ocasiones donde se ha tenido incidentes con equipos que resultaron ser infectados con virus que encriptaron toda la información. La búsqueda del SGSI permitirá fortalecer las políticas, practicas, medidas, y procedimientos disponibles para hacer frente a los riesgos con mayor propiedad.

Con el ideal de planificar y lograr el SGSI se buscará lineamientos que busque abarcar la certificación en salud con respecto a la gerencia de la información, siendo un plus y obtener ventajas competitivas que le permitirá a la institución, tener el grado de reconocimiento nacional e internacional.

Para este proyecto se explorará y estudiara a fondo el estándar de gerencia de la información que es uno de los componentes de la acreditación de salud[4], para poder determinar el alcance sobre qué elementos se estarían cumpliendo.

La metodología que se pretende utilizar es la guía del PMBOK[5] es un instrumento dado por PMI (Project Manager Institute) donde encontramos las mejores prácticas para la planificación de proyectos, mediante sus grupos de procesos y áreas del conocimiento que permitirá alcanzar las metas arrojando un esquema a seguir para la posterior realización e implementación del proyecto planteado.

Este proyecto pretende planificar un Sistema De Gestión De La Seguridad De La Información incorporando las mejoras prácticas del PMBOK donde como resultado se obtendrá un documento con la información guía necesaria para planificar la gestión del SGSI.

Este proyecto nos permitirá aplicar los conocimientos aprendidos en los cursos de la especialización de Seguridad Informática, adquirir más conocimientos de herramientas y

---

[4] http://www.acreditacionensalud.org.co/
[5] Guía de los fundamentos para la dirección de proyectos quinta edición Project Management Institute.

soluciones existentes en el mercado y lograr mayor acercamiento a las normas nacionales e internacionales.

1.4 OBJETIVOS

1.4.1 GENERAL

Diseñar un plan de gestión basado en la guía PMBOK para un Sistema de Gestión de la Seguridad de Información para la Clínica Medical Duarte.

1.4.2 ESPECÍFICOS

Diagnosticar y analizar la situación actual de la institución con respecto al SGSI.

Determinar el marco normativo para la gestión propuesta en la guía del PMBOK.

Determinar y definir el alcance del proyecto para la gestión de la guía PMBOK.

Establecer los planes de gestión de la guía PMBOK determinados por el alcance del proyecto.

1.5 MARCO REFERENCIA

1.5.1 Antecedentes

Para poder realizar una planificación sobre un Sistema de Gestión de la Seguridad de la Información (SGSI), se recomienda conocer otras fuentes de información tanto nacionales como internacionales si fuera posible. Con respecto a un SGSI tomamos como referencia el proyecto de la Ing Paula Andrea Maya Arango, con su trabajo “Plan de Implementación del SGSI Basado en la norma NTC ISO 27001:2013. Donde describe los objetivos, el alcance, la expectativa que tiene con respecto al SGSI, la metodología relacionada a la definición, planeación, identificación y creación de módulos de seguridad para la organización por la cual proyecto el desarrollo del

trabajo. Este proyecto tiene como objetivo sentar las bases del proceso de mejora continua y plantear las acciones necesarias para minimizar el impacto de los riesgos potenciales, planteando las bases para la implementación del SGSI cuyos enfoques son dirigidos a los procesos de las áreas de: división informática, control interno, administración servicios al personal, seguridad física. Para lograr ello planteo la elaboración del proyecto en fases: documentación y normatividad en las mejores prácticas de seguridad de la información. Definición de la situación actual y los objetivos del SGSI de la empresa seleccionada. Análisis de riesgos, junto con la guía Magerit, evaluación del nivel de cumplimiento del IS 27002. Propuesta de para la gestión de la seguridad y el documento con el esquema de seguridad de la información.

Con el estudio de Cobit podemos ayudarnos para organizar la relación de beneficios, recursos, riesgos de las TI. Con Cobit 5 se permite gestionar y gobernar la organización, considerando el negocio, áreas internas y externas. Por lo tanto, sus principios están en satisfacer las necesidades del accionista, tomar toda la empresa para su trabajo, aplicación de un modelo de referencia integrado como único, enfoque holístico y separar gobierno de la gestión.

Tenemos por otra parte con relación a la metodología seleccionada para realizar la planificación del proyecto basado en las buenas prácticas del PMBOK como referencia los especialistas Kelly Tatiana Arroyave Tamayo y Christian Alexander torres Urrea, con el título Formulación Y Diseño De Un Proyecto Basado En La Guía Del PMBOK Para La Interoperabilidad De La Historia Clínica: Caso Christus Sinergia Clínica Palma Real, dado que está relacionado con una institución de salud, donde se enfoca en una investigación cualitativa y estudio descriptivo, identificando causas mediante la metodología del marco lógico, diseñando las fases de inicio y planificación consideradas en la guía del PMBOK V.5., para lograr la interoperabilidad de la historia clínica de los usuarios de la clínica de dicho proyecto.

1.5.2 Marco Teórico

La NTC ISO 27001:2013 norma por excelencia para establecer requisitos, alcanzar su implementación, mantenerlo y mejorar un sistema de gestión de seguridad de la información es su principal menta. Este estándar publicado en el 2005 y aceptado a nivel mundial para la

gestión de la seguridad y su evolución a través de los años con su madurez y confiabilidad pasando por muchos expertos en el área de la seguridad para dar forma a lo que hoy en día se confirma la versión NTC ISO 27001:2013.

Con la implementación de un SGSI podemos estar abarcando puntos importantes del Manual de Acreditación en Salud Ambulatoria y Hospitalaria, se tomará esta guía, uno de sus estándares de acreditación siendo este el grupo de Gerencia de la Información que permitirá dar un enfoque en la integración de todas las áreas asistenciales y administrativas en relación con la información clínica y administrativa y su uso para la toma de decisiones en cualquier nivel de la organización. Cumplir con este estándar se logra que los procesos institucionales cuentes con la información necesaria para la toma de decisiones basada en hechos y datos, implementación de estrategias y mecanismos para garantizar la seguridad y confidencialidad de la información, sistemas de evaluación y mejoramiento de la gerencia de la información, políticas y estrategias para el uso de nuevas tecnologías para el manejo de la información, políticas y estrategias en el manejo de registros clínicos para su disponibilidad en los actores responsables de la salud, definición de planes de contingencia en caso de fallas en sistemas primarios. Se pretende obtener mejores resultados en el desempeño de la gestión de información.

El Ministerio de Tecnología de la Información y las Comunicaciones (MinTIC), con el deseo de fortalecer la gestión TI ha publicado el modelo de seguridad y privacidad de la información (MSPI)[6] donde recopila las buenas prácticas de seguridad, reuniendo los cambios técnicos de la norma 270001 del 2913, nuestras leyes de protección de datos, trasparencia y acceso a la información donde se debe tener presente para la gestión de la información. MSPI posee guías que ayudaran a las entidades a cumplir lo solicitado para cada fase del modelo con miras y lineamientos al protocolo IPv6 en nuestro país. Para nuestro trabajo y aprendizaje adoptaremos este modelo, dado las necesidades y requisitos para nuestros procesos y estructuras con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos de información.

[6] Fortalecimiento de la Gestión TI en el Estado. http://www.mintic.gov.co/gestionti/615/w3-article-5482.html

El cibercrimen es una dura realidad, y debemos estar preparados o prevenidos, una alteración en la funcionalidad de los activos de cualquier índole puede generar traumas para el personal que ha estado acostumbrado en los últimos años a la utilización de elementos informáticos. En el tercer trimestre del 2017, los estudios lograron demostrar que los ataques dirigidos han sido promulgados por agentes del habla china, rusa, inglesa y coreana. Aunque los criminales chinos han estado activos con mayor aumento. Estas amenazas evolucionan constantemente, ya que los ciberdelincuentes están cada vez más preparados, avanzados, tecnológicamente actualizados. Estos aumentos de ataques nos obligan a estar preparados e invertir en inteligencia sobre amenazas y en dotar a las organizaciones con información sobre las más recientes tendencias y acontecimientos[7].

Una de las grandes casas de soluciones en software de seguridad, ESET fundada en 1992, en su informe del 2017, muestra la preocupación entre las empresas de 13 países y 4000 ejecutivos y profesionales de la TI de estos países donde se resume en el siguiente cuadro según el tamaño de empresas, por los 2 últimos años y los ataques más comunes a nivel mundial.

Gráfico comparativo ataques y preocupaciones de acuerdo con el tamaño de empresa.

Tabla 1 **Ataques y preocupaciones**

Empresas	Año	Malware	Fraude	Vulnerabilidad de software y sistemas	Ataque de denegación de servicio	Phishing	Acceso indebido a la información
Grandes	2015	52%	38%	60%	37%	34%	46%
	2016	55%	29%	53%	28%	28%	36%
Medianas	2015	60%	35%	60%	32%	34%	50%
	2016	56%	25%	49%	21%	27%	38%
Pequeñas	2015	55%	39%	58%	26%	28%	45%
	2016	57%	32%	51%	15%	22%	30%

[7] Informe 2017 comunicado de prensahttps://latam.kaspersky.com/about/press-releases/2017_half-of-targeted-attacks-q3-2017-chinese-origin

Fuente: ESET[8].

También se debe destacar las modalidades de protección que optan las empresas, entre los cuales se encuentras los controles de seguridad, la gestión de esta, educación y concientización, distribuir la responsabilidad en seguridad y el presupuesto que ello implica.

En importante primero planificar nuestros actos y luego pasar a la ejecución, esto permitirá seguir unas pautas que nos llevará a culminar con proyectos exitosos. Los lineamientos del PMBOK (Project Management Body of Knowledge), como un estándar de PMI (Project Management Institute) que tiene la bondad de recopilar las mejores prácticas para dirigir proyectos, para describir normas, métodos, prácticas y procesos para dirigir el proyecto. En este se encuentra establecido la dirección de proyecto mediante 5 grupos claves de procesos y sus interacciones, siendo estos los procesos de Inicio, Planificación, Ejecución, Monitoreo – Control y Cierre. A su vez las 10 áreas del conocimiento que ofrece la guía del PMBOK, donde se agrupan 47 procesos para la dirección del proyecto, están conformados por un ámbito profesional, de la dirección o un área especializada, representando un conjunto completo de conceptos, términos y actividades, cada área se trata de una sección específica del PMBOK. Uno de los grandes líderes en las misiones espaciales como lo es la NASA, ha puesto en práctica la gestión de proyectos PMI, convirtiéndola en una de las herramientas más importantes en toda la organización[9]. El desastre del Challenger los llevo a tomar la firme decisión de cambiar la organización hacia la excelencia en la gestión de proyectos con el objetivo formado en su personal, fomentando el aprendizaje de la experiencia de sus ingenieros y profesionales de mayor éxito, buscando nuevos conocimientos y sinergias con el exterior. Para la NASA, PMI le yudo enormemente a ganar memoria de sus proyectos, planificar mejor, optimizar los recursos, y responder al exigente escenario de los últimos años en el que ha habido que trabajar más rápido, mejor, más barato, y todo ello experimentando reducciones sustanciales de personal y

[8] ESET Security Report. ESET Security Report Latinoamérica (2017). Recuperado de: https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf
[9] NASA, caso de éxito en gestión de proyectos PMI http://itcformacionyconsultoria.com/nasa-gestion-de-proyectos-pmi/

presupuesto. Según Dr. Hoffman director de proyecto – PMP dice ver en el PMI y la Guía del PMBOK el mapa del plan gestión de proyectos. "Se adapta a nuestras necesidades generales, pero también a las específicas de áreas como ingeniería, seguridad de materiales, etc."

Otros casos de existo en América Latina en la utilización de PMI, se encuentra la construcción de 4 estadios en 9 meses para el mundial femenino sub-20 en chile, central hidroeléctrica platanal en Perú en tiempo record. Programa de expansión del canal de panamá[10].

El Sistema de Gestión de la Seguridad de la Información es una parte del sistema de gestión general, basada en un enfoque de riesgos empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información[11]. Su uso se ve reflejado en las mejoras prácticas para conocer y controlar los riesgos para los que están sometidos los datos y fuentes de información, se asumen, minimizan, transfiere o controla.

Parte fundamental de nuestro trabajo está relacionado con la NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001, donde se tomará dicha norma como base fundamental para poder proyectar e implementar las 10 áreas del conocimiento o las seleccionadas según el alcance del proyecto direccionando de forma planificada cada requerimiento solicitado por la norma.

COBIT ha sido aceptado a nivel mundial, entidades bancarias, grupos empresariales han adoptado y utilizado este método. Internacionalmente el ministerio de recursos humanos de sultanato de oman, impulsaron proyectos e iniciativas de gobierno electrónico, junto con el departamento de seguridad de red e informática del ministerio. Sus implementadores de ingeniería de procesos recomendaron Cobit 5 y sus 5 principios como una solución para la implementación de GEIT.

---

[10] Buchtik L., proyectos exitosos en América Latina (2010) http://americalatina.pmi.org/~/media/Files/latam/Argentina-Capitulo-Nuevo-Cuyo/2011-AR-NC-Buchtik-ProyectosExitosos.aspx

[11] Josue Sorto, Sistema de Gestión de Seguridad Informática SGSI (2017). https://es.slideshare.net/joelsorto96/sistemas-de-gestin-de-seguridad-informtica-sgsi

En Colombia también se han generado esfuerzos para su utilización, siendo Ecopetrol una empresa energética, decidida a transforma corporativamente sus objetivos de crecimiento para buscar un enfoque en la gobernanza y gestión de los servicios TI, logrando consolidar una sólida gobernanza de TI, cuyas practicas lograron alinear sus iniciativas corporativas de control interno. Ecopetrol selecciono Cobit para su marco de gobierno TI pro el mapeo de objetivos de TI a objetivos comerciales, mejor alineación basado en un enfoque comercial, visión sobre las actividades TI, responsabilidades basadas en la orientación al proceso, aceptación de entidades reguladoras y terceros, entre otros. En su uso y proceso de sostenibilidad jugaron papel importante factores como clave de éxito los resultados de confiabilidad de la información, confianza TI, integralidad organizacional, evaluación continua, cultura organizacional y el apoyo a los servicios de consultoría.

La ISO 31000, permite complementar nuestro proyecto para el análisis y evaluación de riesgos mediante buenas prácticas internacionales para alcanzar una eficiente gestión del riesgo. Lo anterior se traduce en un incremento de la seguridad dado por su enfoque basado en riesgos. Para aumentar el grado de éxito, el Sistema de Gestión de riesgo debe ser integrado, estructurado, adaptado, inclusivo, dinámico, información amplia y certera, revisar los factores humanos y culturales, por último, la mejora continua debe incluirse.

La ISO / IEC – Estándar 13335: 2014, con técnicas de seguridad, con sus conceptos y modelos para la gestión de la tecnología. Este nos dará pautas y recursos para la implementación de prácticas de gestión de seguridad y criterios para auditar.

La ISO 17799 esta norma técnica peruana nos permitirá implementar medidas de seguridad dentro de la organización. Esta da soporte y dirige la gestión de la seguridad de la información.

1.5.3 Marco Conceptual

La Guía de los Fundamentos para la Dirección de Proyectos. *(Guía del PMBOK®)* - Quinta Edición proporciona pautas para la dirección de proyectos individuales y define

conceptos relacionados con la dirección de proyectos. Describe asimismo el ciclo de vida de la dirección de proyectos, los procesos relacionados, así como el ciclo de vida del proyecto.

Qué es la Dirección de Proyectos: para cumplir con los requisitos de este debemos aplicar conocimientos, habilidades, herramientas y técnicas a las actividades del proyecto. Para lograr ello debemos lograr la aplicación e integración adecuadas de los 47 procesos de la dirección de proyectos.

NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001:2013: siendo el INCONTEC una entidad privada, sin ánimo de lucro, cuya misión es fundamental para brindar soporte y desarrollo al productor y protección al consumidor, para lograr ventajas competitivas en los mercados internos y externos. La norma tiene el propósito de establecer, implementar, operar, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información.

Parte fundamental para nuestro trabajo es conocer la documentación del Sistema Gestión de Seguridad de la Información, siendo este aspecto el principal objetivo de estudio en cuyo caso debemos hacer uso de encuestas, entrevistas, observación directa para poder recolectar información y elaborar nuestro proyecto. Se considera que el problema de la institución es contener mucha información plasmada en papel que han dado solución a elementos particulares pero que no se logra tener claro la magnitud y escala de este para que puedan contribuir con la filosofía de la acreditación en salud.

- Fundamentos de la Dirección de Proyectos

La guía de fundamentos para la dirección de proyecto proporciona pautas para la dirección de proyectos individuales y define conceptos relacionados con la dirección de proyectos.

Entendemos como proceso a un esfuerzo que se lleva a cabo para crear un producto, servicio o resultado único durante un tiempo planificado, bajo la naturaleza de tener un principio y un final definidos. Al lograr los objetivos se alcanza el final, en el mejor de los escenarios, pero también

puede finalizar por no lograrse los objetivos, finalización de las partes, incumplimientos o se perdió la necesidad que dio origen al proyecto.

Entre tanto la dirección de proyecto se aplica al conocimiento, habilidades, herramientas y técnicas sobre las actividades del proyecto para cumplir con los requisitos. La dirección de proyectos del PMI aplica e integran 47 procesos, congregados en 5 grupos de procesos que veremos más adelante.

Se debe tener presente en la estructura de la dirección de proyecto la influencia que puede lograr adquirir las entidades externas, como también la cultura, estilo y estructura de la organización.

Un término concurrente en la dirección del proyecto son los interesados, siendo estos los principales benefactores, pero también posibles afectados por las decisiones, actividades o resultado del proyecto. Los interesados pueden tener influencia sobre el proyecto, los entregables.

En cuanto a la gobernabilidad del proyecto permite dirigir los proyectos de manera coherente, maximizar el valor de sus resultados y alinear los mismos con la estrategia del negocio. Permitirá tomar decisiones para satisfacer las necesidades y expectativas de los interesados como los objetivos estratégicos de la organización.

La frase de “ciclo de vida de un proyecto” es la serie de fases acotadas en el tiempo con inicio y final o punto de control por la que atraviesa un proyecto desde su inicio hasta su cierre. Las llamadas fases se dividen en objetivos funcionales o parciales, resultados o entregables intermedios, hitos específicos del alcance global del trabajo o disponibilidad financiera.

- Grupo de procesos

Grupo Proceso de Inicio: se compone por procesos para iniciar un proyecto o fase. En este se define el alcance, recursos financieros, identifica interesados y demás parámetros que dicta cada proceso que lo compone.

Grupo de Procesos de planificación: contiene procesos para establecer el alcance total del esfuerzo, definir y refinar objetivos junto con las líneas de acción para lograrlos, retroalimentación del ciclo del proyecto para calcular la planificación adicional que lo requiera.

Grupo de Proceso de Ejecución: lo componen aquellos procesos para completar el trabajo definido en el plan para la dirección del proyecto con el fin de cumplir con las especificaciones de este. Este grupo implica coordinar personas, recursos, gestionar las expectativas de los interesados e integrar y realizar las actividades del proyecto conforme al plan trazado.

Grupo de procesos de monitoreo y control: lo componen los procesos requeridos para analizar y dirigir el progreso y el desempeño del proyecto de tal forma que se logre identificar áreas en las que el plan requiera cambios y para iniciar los cambios correspondientes.

Grupo de procesos de Cierre: son procesos para finalizar las actividades de todos los grupos de procesos de la dirección de proyectos con el fin de completar formalmente el proyecto, fases u otras obligaciones contractuales.

- Lineamientos guía PMBOK.

Para nuestro trabajo haremos uso de las mejores prácticas para la Dirección de Proyectos, siendo la Guía PMBOK un estándar para dirigir proyectos para diversos tipos de industrias. Para lograr un resultado exitoso, la guía describe 5 procesos, 10 áreas del conocimiento y 47 procesos para la dirección de proyectos:

Tabla 2 Resumen Grupo de Procesos PMBOK

Grupo de proceso	Descripción	Procesos
Proceso de Inicio	Posee aquellos procesos para definir un nuevo proyecto o nuevas fases en proyectos existentes para obtener la autorización e iniciar el proyecto. Ayuda a establecer una visión del proyecto	2

Procesos de Planificación	Procesos que permitirá establecer el alcance del proyecto, objetivos, definir el curso de acciones necesario para alcanzar los objetivos.	24
Procesos de Ejecución	Procesos para contemplar el trabajo definido en el plan para la dirección del proyecto con el fin de cumplir con las especificaciones del mismo.	8
Procesos de Monitoreo y Control	Procesos para monitorear, analizar y regular el progreso y el desempeño del proyecto, identificar e iniciar los cambios que requieren las áreas.	11
Procesos y Cierre	Procesos para finalizar todas las actividades de todos los grupos de procesos con el fin de cerrar formalmente el proyecto o una fase de este.	2
	TOTAL PROCESOS:	47

Fuente: extracción ideas generales en la guía PMBOK

Los resultados que cada grupo de procesos producen permite la vinculación entre ellos. Cada grupo cuenta con dependencia bien definida y elevada interacción entre sí.

Dados los tiempos que tenemos para la presentación del proyecto de grado, nos fijaremos como limites en el estudio y elaboración de los procesos necesarios de los grupos de proceso de inicio y planificación. Para ello estudiaremos los procesos que componen estos dos grupos.

Para comprender la filosofía que plasma la guía PMBOK con respecto a las 10 áreas del conocimiento, los 5 grupos de procesos y sus 47 procesos, veremos a continuación un resumen de estos plasmados en la guía.

Tabla 3 Relación Grupos de Procesos y Áreas de conocimiento

	GRUPOS DE PROCESOS y áreas del conocimiento de la dirección de proyecto.				
Áreas de Conocimiento	Grupo de Procesos de Inicio	Grupo de Procesos de Planificación	Grupo de Procesos de Ejecución	Grupos de Procesos de Monitoreo y control	Grupo de procesos de cierre

4. Gestión de la Integración del Proyecto	4.1 Desarrollar el acta de constitución del proyecto	4.2 Desarrollar el plan de dirección del proyecto	4.3 Dirigir y gestionar el trabajo del proyecto	4.4 Monitorear y controlar el trabajo del proyecto 4.5. Realizar el control integrado de cambios	4.6. Cerrar proyecto o fase
5. Gestión del Alcance del Proyecto		5.1. planificar la gestión del alcance 5.2. recopilar requisitos 5.3 crear la ETD/WBS		5.5 validar el alcance 5.6. controlar el alcance	
6. Gestión del tiempo del proyecto		6.1 Planificar la gestión del cronograma 6.2. definir las actividades 6.3. secuenciar las actividades 6.4. estimar los recursos de las actividades 6.5. estimar la duración de las actividades 6.6. Desarrollar el cronograma		6.7. controlar el cronograma	
7. Gestión de los costes del proyecto		7.1 planificar la gestión de los costos 7.2. estimar los costos 7.3 determinar el presupuesto		7.4 controlar los costos	
8. Gestión de la calidad del proyecto		8.1 planificar la gestión de la calidad	8.2 realizar el aseguramiento de calidad	8.3 controlar la calidad	
9. Gestión de los recursos Humanos del Proyecto		9.1 planificar la gestión de los recursos humanos	9.2 adquirir el equipo del proyecto 9.3. desarrollar el equipo del proyecto 9.4. dirigir el equipo del proyecto		
10. Gestión de las comunicaciones del proyecto		10.1 planificar la gestión de las comunicaciones	10.2 gestionar las comunicaciones	10.3 controlar las comunicaciones	
11. Gestión de los riesgos del proyecto		11.1. planificar la gestión de los riesgos 11.2 identificar los riesgos 11.3. realizar el análisis cualitativo de riesgos 11.4 realizar el análisis cuantitativo de riesgos 11.5 planificar la respuesta a los riesgos		11.6 controlar los riesgos	
12. Gestión de las adquisiciones del proyecto		12.1. planificar la gestión de las adquisiciones	12.2. efectuar las adquisiciones	12.3 controlar las adquisiciones	12.4 cerrar las adquisiciones
13. Gestión de los interesados del proyecto	13.1 identificar los interesados	13.2. planificar la gestión de los interesados	13.3 gestionar la participación de los interesados	13.4 controlar la participación de los interesados	

Fuente: guía PMBOK[12].

Desarrollar el Acta de Constitución del proyecto:

Punto de partida para todo proyecto basado en la guía del PMBOK. Se realizará un documento que autoriza formalmente la existencia de un proyecto y confiere al director del proyecto la autoridad para asignar los recursos de la organización a las actividades del proyecto.

[12] PMBOK GUIDE, sixth Edition https://www.pmi.org/pmbok-guide-standards/foundational/pmbok

Identificar a los Interesados:

Permite identificar las personas, grupos u organizaciones que podrían afectar o ser afectados por una decisión, actividad o resultado del proyecto, analizar y documentar información relevante de sus intereses, participación, interdependencias, influencia e impacto para el éxito del proyecto.

Desarrollar el plan Para la Dirección del Proyecto:

Mediante este procedo definiremos, prepararemos y coordinaremos todos los planes secundarios e incorporados en un plan integral para la Dirección del proyecto. Su beneficio clave es un documento central que define la base para todo el trabajo del proyecto.

Planificar la Gestión del Alcance:

Este proceso nos permitirá crear un plan de gestión del alcance que documente cómo se va a definir, validar y controlar el alcance del proyecto. Su beneficio es proporcionar una guía y dirección sobre cómo se gestionará el alcance a lo largo del proyecto.

Recopilar Requisitos:

Permite determinar, documentar y gestionar las necesidades y los requisitos de los interesados para cumplir con los objetivos del proyecto.

Definir el Alcance:

Desarrolla una descripción detallada del proyecto y del producto.

Crear la EDT / WBS:

Este proceso subdivide los entregables y el trabajo del proyecto en componentes más pequeños y fáciles de manejar.

Planificar la Gestión del Cronograma:

Proceso por medio del cual se establecen las políticas, procedimientos y la documentación para planificar, desarrollar, gestionar, ejecutar y controlar el cronograma del proyecto. Su beneficio clave radica es proporcionar la guía y dirección sobre cómo se gestionará el cronograma del proyecto a lo largo del mismo.

Definir las Actividades:

Proceso de identificar y documentar las acciones específicas que se deben realizar para generar los entregables del proyecto. Su beneficio es el desglose de los paquetes de trabajo en actividades que proporcionan una base para la estimación, programación, ejecución, monitoreo y control del trabajo de proyecto.

Secuenciar las Actividades:

Identificar y documentar las relaciones existentes entre las actividades del proyecto. Su punto clave está en la definición de la secuencia lógica de trabajo para obtener la máxima eficiencia teniendo en cuenta todas las restricciones del proyecto.

Estimar los Recursos de las Actividades:

Estimar el tipo y las cantidades de materiales, recursos humanos, equipos o suministros requeridos para ejecutar cada una de las actividades. Con este nos beneficia para estimar el costo y la duración de manera más precisa.

Estimar la Duración Actividades:

Estimar la cantidad de periodos de trabajo necesarios para finalizar las actividades individuales con los recursos estimados. Su punto clave es que permite establecer la cantidad de tiempo necesario para finalizar cada una de las actividades y cuales constituyen entradas fundamentales para el proceso de desarrollar el cronograma.

Desarrollar el Cronograma:

Proceso para analizar secuencias de actividades, duración, requisitos de recursos y restricciones del cronograma para crear el modelo de programación del proyecto. Esto genera un modelo de programación con fechas planificadas para completar las actividades del proyecto.

Planificar la Gestión de los Costos:

Proceso para establecer políticas, los procedimientos y la documentación necesaria para planificar, gestionar, ejecutar el gasto y controlar los costos del proyecto. Su beneficio clave es proporcionar guía y dirección sobre cómo se gestionarán los costos del proyecto a lo largo del mismo.

Estimar los Costos:

Este proceso consiste en desarrollar una aproximación de los recursos financieros necesarios para completar las actividades del proyecto. Su beneficio radica en determinar el monto de los costos requeridos para completar el trabajo del proyecto.

Determinar el Presupuesto:

Este proceso consiste en sumar los costos estimados de las actividades individuales o de los paquetes de trabajo para establecer una línea base de costo autorizada. Podemos monitorear y controlar el desempeño del proyecto.

Planificar la Gestión de la Calidad:

Proceso para identificar los requisitos y/o estándares de calidad para el proyecto y sus entregables, así como de documentar como el proyecto demorara el cumplimiento con los mismos. Proporcionará una guía y dirección sobre cómo se gestionará y validará la calidad a lo largo del proyecto.

Planificar la Gestión de los Recursos Humanos:

Este proceso identifica y documenta los roles dentro de un proyecto, responsabilidades, habilidades requeridas, organigrama y las relaciones de comunicación, también crear un plan para la gestión del personal. Está relacionado con el cronograma de adquisición y liberación del personal.

Planificar la Gestión de las Comunicaciones:

Permite desarrollar un enfoque y un plan adecuado para las comunicaciones del proyecto con base a las necesidades y requisitos de información de los interesados y de los activos de la organización disponibles. Permite identificar y documentar el enfoque a utilizar para las comunicarse con los interesados de la manera más eficaz y eficiente.

Planificar la Gestión de los Riesgos:

Define como realizar las actividades de gestión de riesgos de un proyecto. Permitirá asegurar que el nivel, tipo y la visibilidad de la gestión de riesgos son acordes tanto con los riesgos como la importancia del proyecto para la organización.

Identificar los Riesgos:

Determinar los riesgos que pueden afectar al proyecto y documentar sus características. Permite documentar los riesgos existentes, el conocimiento y la capacidad que confiere al equipo del proyecto para anticipar eventos.

Realizar el Análisis Cualitativo de Riesgos:

Priorizar riesgos para análisis o acción posterior, evaluando y combinando la probabilidad de ocurrencia e impacto de dichos riesgos. Permitirá a los directores de proyecto reducir el nivel de incertidumbre y concentrarse en los riesgos de alta prioridad.

Realizar el Análisis Cuantitativo de Riesgos:

El análisis numérico del efecto de los riesgos identificados sobre los objetivos generales del proyecto. Su beneficio genera información para la toma de decisiones a fin de reducir la incertidumbre del proyecto.

Planificar la Respuesta a los Riesgos:

Proceso para desarrollar opciones y acciones para mejorar las oportunidades y reducir las amenazas a los objetivos del proyecto. Aborda los riesgos en función de su prioridad, introduciendo recursos y actividades en el presupuesto, cronograma y plan de dirección de proyecto según las necesidades.

Planificar la Gestión de las Adquisiciones:

Documentar las decisiones de adquisiciones del proyecto, especificar el enfoque e identificar a los proveedores potenciales. Nos permite determinar si es preciso obtener apoyo externo y, si fuera el caso, que adquirir, de qué manera, en que cantidad y cuando hacerlo.

Planificar la Gestión de los Interesados:

Desarrollar las estrategias de gestión adecuadas para lograr la participación eficaz de los interesados a lo largo del ciclo de vida del proyecto, con base al análisis de sus necesidades, intereses y el posible impacto en el existo del proyecto. Proporciona un plan claro y factible para interactuar con los interesados del proyecto con el fin de apoyar los intereses de este.

1.5.4 Marco Legal y Jurídico

La norma ISO 27001[13], entiende la importancia de los activos en general, para el buen desarrollo operativo, de control, gestión de modelo de negocio para cualquier organización. Esta especifica los requisitos para establecer, implementar, documentar y evaluar un Sistema de Seguridad de la Información. Es importante seguir las actividades que este ofrece, tales como definir el alcance, las políticas, metodologías y criterios para el análisis y gestión de riesgos, identificarlos, evaluar y desarrollar el tratamiento de estos. Además, elaborar una declaración de aplicabilidad de controles y requisitos; debemos acompañar lo anterior con el desarrollo de programas de formación y concienciación en SI, gestionar los recursos y operaciones, de incidencias y elaborar los procesos y su documentación asociada.

Para las instituciones de salud principalmente se rige por la resolución 1995 de 1999, donde se establecen las normas para el manejo de la Historia Clínica, La ley 100 de 1993 donde se faculta al ministerio de salud para dictar las normas científicas que regulan la calidad de los servicios, de obligatorio cumplimiento por parte de todas las entidades promotoras de salud, prestadores de servicios de salud del sistema general de seguridad social en salud y las direcciones seccionales, distritales y locales de salud.[14]

---

[13] http://www.gesconsultor.com/iso-27001.html

[14] https://www.minsalud.gov.co/Normatividad_Nuevo/RESOLUCI%C3%93N%201995%20DE%201999.pdf

1.6 MARCO METODOLÓGICO

Este proyecto contempla la utilización de la metodología dada por el Project Manager Institute guía PMBOK[15] como metodología principal para el desarrollo del proyecto. También exploraremos el documento de buenas prácticas nacionales e internacionales para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo mediante el Modelo de Seguridad y Privacidad de la información – MSPI[16] de la estrategia de Gobierno En Línea (GEL), siendo una fuente de información y documentación estratégica para el avance del proyecto.

1.6.1 Fuentes de información

Entre las cuentas las fuentes primerias tenemos la inspección directa, entrevistas directa de los funcionarios o colaboradores principales del Departamento de Sistemas o lista de chequeo. La fuente de información secundaria para soportar la investigación se revisará con la guía del PMBOK. Una última fuente alternativa para referenciar dado por las buenas prácticas que otorga el ministerio de las TIC Colombia mediante MSPI, cuyos lineamientos están en el marco de referencia de arquitectura TI, soportando los componentes de la Estrategia En Línea. Debemos tomar en consideración el estudio de las normas y Controles que ofrece la NTC ISO 27001:2013, ISO 31000 y 27002:2013 como fuente primordial y guía para todo el Sistema de Gestión de la Seguridad de la Información que se pretende planificar.

1.1.1 [15] PMI | Project Management Institute

[16] Ministerio de Tecnología de la Información y las Telecomunicaciones. Rescatado de: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

1.6.2 Tipo de Investigación

El tipo de investigación será dada de tipo cuantitativo, posterior a la recopilación de encuestas, cuestionarios y/o entrevista con los actores encargados tanto en el departamento de sistemas como del Sistema de Gestión de Calidad, con el fin de determina el avance que posee la institución con respecto al SGSI[17], para determinar el nivel de madurez o avances con respecto a dicho sistema.

1.6.3 Método de Investigación

Se tendrá en cuenta: A) la información de la institución y su marco normativo. B) La recopilación de información de la institución permitirá analizar y diagnosticar la situación actual del mismo con respecto al SGSI. C) conocer la iniciativa que la institución requiere para lograr la acreditación da un fundamento inicial para el proyecto en su necesidad de buscar la excelencia con un sistema de gestión que le permita lograr la confidencialidad, integridad y disponibilidad de la información de forma mucho más certera, estructurada y organizada desde todos los puntos de vista medibles que la institución requiere implementar.

1.6.4 Población y muestra

La población objeto de estudio está conformada por los departamentos de sistemas, calidad, redes y telecomunicaciones. La muestra entre dichos grupos es pequeña:

[17] Sistema de Gestión de la Seguridad de la Información – Norma ISO 27001.

Tabla 4 **Población / Muestra**

Población	Muestra
Sistemas	3
Calidad	3
Redes y telecomunicaciones	2

Fuente: propia.

—

Para la recolección de datos se hace uso de entrevistas, además de la experiencia de trabajar dentro de la institución.

Fases metodológicas

1.7 FASE 1. SITUACIÓN ACTUAL.

1.7.1 La institución.

La Clínica Medical Duarte ZF S.A.S (CMD), es una institución joven prestadora de salud, a 3 años de su inauguración, con nivel de complejidad 3, buscando la acreditación en salud y mejorando cada día sus procesos con el fin de prestar el mejor servicio para la mayor satisfacción de nuestros pacientes.

El departamento de sistema tiene la tarea de gestionar la administración de los sistemas asistencial (Historias Clínicas), Financieros, Glosas, Jasper, Parqueadero, Siau, como también la administración de la Base de Datos Asistencial, glosas. Diseñar y crear reportes para el sistema Jasper. Gestionar el servicio de impresoras y otras actividades inherentes al departamento.

La institución posee una gran gama de activos entre los cuales se encuentra aproximadamente 350 computadores y portátil (y creciendo este activo dado los servicios abiertos en el último mes), Router, Swicth, redes categoría 7, telefonía IP, 6 servidores, ups, Data Center, sistemas eléctricos, sistemas contra incendio, llamados de enfermería, etc. y demás componentes que por ley son requeridos.

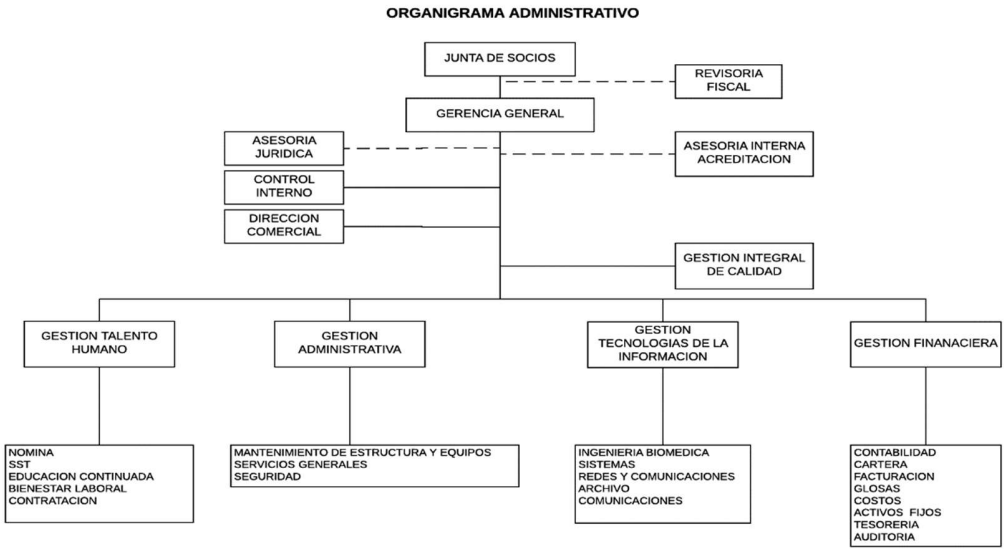


Imagen 1 Organigrama Administrativo

La Clínica Medical Duarte ZF S.A.S, ha invertido un gran esfuerzo en recursos humanos, tecnológicos y económicos para fortalecer a diario los procesos que conllevan a la buena atención hacia el paciente con sentido humano, por tal motivo a continuación el siguiente mapa de procesos:

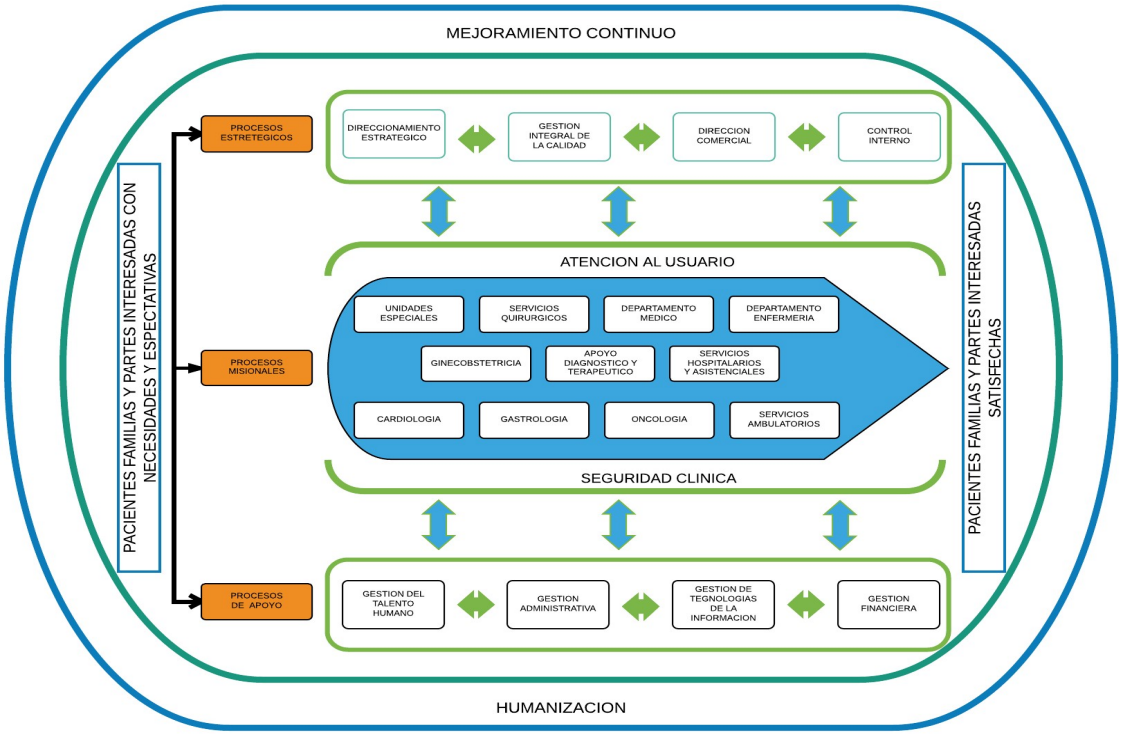


Imagen 2 Mapa de procesos CMD

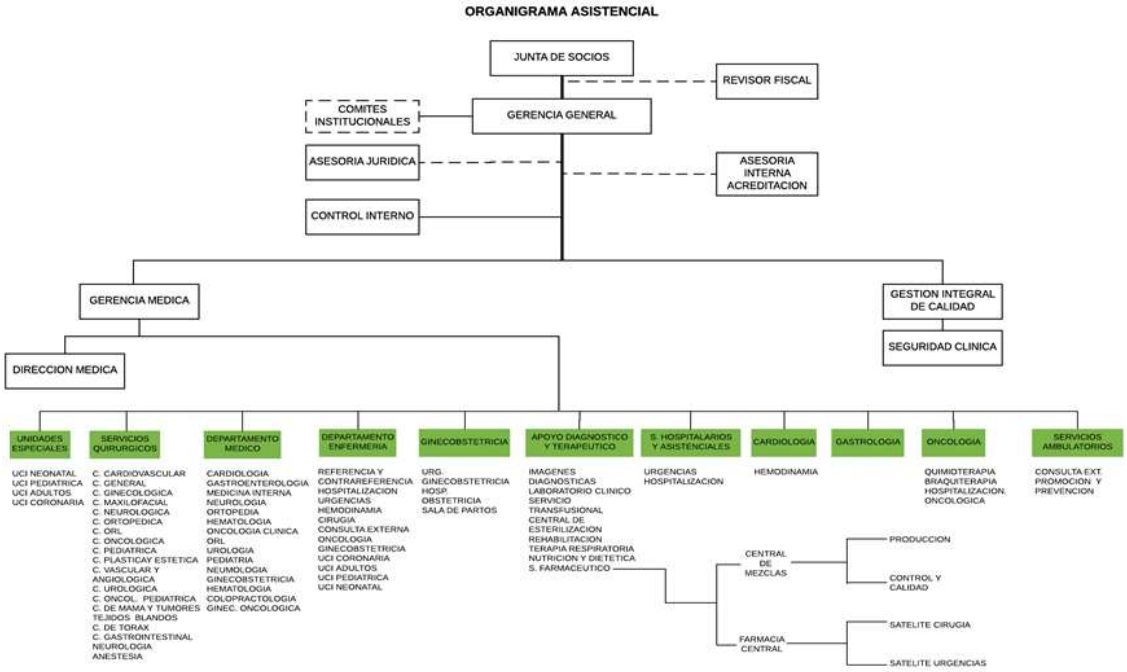


Imagen 3 Organigrama Asistencial CMD

Misión

En la Clínica Medical Duarte Trabajamos por la recuperación de la salud de nuestros pacientes, a través de servicios integrales de Mediana y Alta Complejidad desarrollados con estándares de calidad, de manera segura y humanizada apoyados en un modelo organizacional eficiente, un recurso humano competente y comprometido y una tecnología de vanguardia.

Visión

Para el año 2020 seremos reconocidos como el centro de referencia en servicios de salud de alta complejidad en la región, por su liderazgo en la integralidad, la atención segura y humanizada y los estándares de calidad superiores.

Objetivos Corporativos

Rentabilidad Y Estabilidad Financiera.

Reconocimiento Como Centro De Referencia De Alta Complejidad.

Liderazgo En Atención Integral Segura Y Humanizada.

Alcanzar Estándares De Calidad Superior.

Recurso Humano Competente.

Objetivos de Calidad

Tabla 5 Objetivos de calidad

Satisfacción: Garantizar la satisfacción de las necesidades y expectativas ofreciendo servicios enmarcados en los principios de calidad.	**Calidad:** Garantizar la calidad de la atención en salud mediante la accesibilidad, oportunidad, seguridad, pertinencia y continuidad.
Atención Segura: Fortalecer la implementación de prácticas médicas seguras con los más altos estándares de seguridad.	**Integración:** Lograr la integración sistemática de las unidades de la organización para garantizar la efectividad y eficiencia mediante el mejoramiento continuo de los procesos de calidad.
Innovación: Propender por la innovación tecnológica de la institución y mantener una adecuada infraestructura física, de tal forma que le permita mantener su competitividad y su posición de liderazgo en el sector.	**Formación:** Promover la formación continua e integral que garantice el desarrollo personal del recurso humano, reflejando la calidad y humanización en la atención de nuestros pacientes.
Pertenencia: Transmitir al personal de la clínica la amabilidad y el respeto en la atención de los pacientes, e incentivar el compromiso y responsabilidad por las actividades que realizan día a día.	**Responsabilidad:** Orientar nuestros procesos hacia el cumplimiento de una política de responsabilidad social empresarial comprometida con la generación de valor social y el cuidado del medio ambiente.

Fuente: Sistema Gestión Calidad – Clínica Medical Duarte

Valores Institucionales

Imagen 4 Valores Institucionales

Propuesta de Valores

La Clínica Medical Duarte trabaja por una atención segura, oportuna e integral a sus pacientes en el ámbito médico y quirúrgico, que le permitan una pronta recuperación y satisfacción por los servicios recibidos.

Tabla 6 Competencias Organizacionales CMD

COMPETENCIA: Es la capacidad real para lograr un objetivo o resultado en un contexto dado, según estándares y calidad establecidos, integrando conocimientos, habilidades, destrezas, actitudes, valores y ética, que permite comprender actuar y transformar el mundo que les rodea.	**ETICA:** Capacidad para actuar con valores morales y buenas costumbres, para el cumplimiento de las políticas de la clínica y el bienestar común, aun por encima de los objetivos personales y respetando las diferencias.
RESPONSABILIDAD: Es la conciencia acerca de las consecuencias que tiene todo lo que hacemos o dejamos de hacer sobre nosotros mismos o los demás. La responsabilidad busca siempre hacer nuestro mejor esfuerzo por alcanzar los objetivos empresariales	**TRABAJO EN EQUIPO:** Habilidad para integrarse en a un equipo de trabajo con responsabilidad para alcanzar los objetivos establecidos combinando adecuadamente personas, situaciones y tiempo, emprendiendo acciones eficaces para mejorar el talento, las capacidades propias y las de los demás.
RESPETO: Es la base fundamental para la convivencia sana y pacífica entre los miembros de una sociedad, siendo conscientes del valor propio ser y la dignidad de los demás, para poder comprenderlos y aceptarlos	**COMUNICACIÓN ASERTIVA:** Es la habilidad de expresar los sentimientos o ideas positivas y negativas de una manera abierta, honesta y directa. Que reconoce nuestros derechos al mismo tiempo que sigue respetando los derechos de los otros.
TRATO AMABLE Y HUMANIZADO: Es la forma amable, cordial, y empática, que se pone de manifiesto, durante el proceso de atención, en donde prima el respecto a sus derechos valorando su cultura y condiciones humanas.	

Fuente: Sistema Gestión Calidad – Clínica Medical Duarte

Imagen 5 Principios corporativos

Fuente: Sistema Gestión Calidad – Clínica Medical Duarte

1.7.2 Estado Actual de la Institución

La institución Clínica Medical Duarte, es una institución joven prestadora de salud, pero con el gran anhelo e iniciativa de poder alcanzar los altos estándares de calidad en salud, para lograr ello, en el último año, se ha incluido personal para el área asistencial en las actividades pertinentes para lograr la acreditación en salud. Para Nuestro proyecto es importante conocer el avance actual que posea la institución. Desde el primer levantamiento previo de información a principio de año, con respecto a la fecha del presente documento se ha obtenido algunos avances para la acreditación de forma exploratoria.

El hecho de estar laborando dentro de la institución me da la oportunidad de saber de primera mano la situación actual, y aún más desde el punto de vista de la seguridad informática, que ciertamente se implementan saberes generales que permiten darle continuidad al negocio.

Las inspecciones directas han permitido conocer algunos avances en políticas y otras falencias relacionadas con la seguridad que no permitirían lograr el 100% del objetivo para el Sistema de Gestión de la Seguridad Informática.

Aunque existen algunas políticas creadas dadas las anomalías ocurridas en algunos eventos en particulares, no se ha logrado crear los controles pertinentes para abarcar con mayor amplitud la seguridad de la información.

En la revisión del estándar NTC ISO 27001:2013 y basado en los controles otorgados por la ISO 27002, se realizó una lista de chequeo para explorar los dominios implementados, ejecutados o planificados.

Tabla 7 Lista de chequeo Exploración Dominio ISO 27002

Dominio	Implementado / %	Observación
Políticas de seguridad.	NO / 20	Algunas políticas creadas para dar cumplimiento a superintendencias.
Aspectos organizativos de la seguridad informática.	NO / 0	
Gestión de activos.	NO / 5	Existen algunos controles en la codificación en algunos activos.

Seguridad ligada a los recursos humanos.	NO / 10	Existen algunos procesos en el ingreso del personal.
Seguridad física y del entorno.	NO / 30	Existen algunas áreas que se consideran vulnerables con un grado de seguridad aceptable.
Gestión de comunicación y operaciones.	NO / 10	Algunos controles implementados.
Control de acceso.	NO / 15	Controles implementados para el ingreso en algunas áreas.
Adquisición, desarrollo y mantenimiento de información.	NO / 0	
Gestión de incidentes en la seguridad de la información.	NO / 5	Algunas actividades existen, pero no están documentadas.
Gestión de la continuidad del negocio.	NO / 0	Se realizan actividades importantes para mantener el negocio, pocas estas documentadas.
Cumplimiento.	NO / 0	

Fuente: propia con ideas basadas los ítems de la ISO 27002

1.8 FASE 2. MARCO NORMATIVO GUÍA PMBOK.

Para nuestro proyecto nos basaremos en los procesos de inicio y planificación, además, para el proceso de planificación se estudiará la posibilidad de realizar todos los relacionados en la tabla "Relación Grupos de Procesos y Áreas de conocimiento" para dicho grupo.

1.8.1 Grupo Procesos de Inicio

- Acta de Constitución

Como se explicó con anterioridad, el acta de constitución autoriza formalmente la existencia del proyecto y otras especificaciones registradas en el presente documento. Para ello planeamos diligenciar el siguiente formato

Tabla 8 Acta Constitución

ACTA CONSTITUCION	
NOMBRE DEL PROYECTO	**IDENTIFICADOR**
JEFE PROYECTO	**FECHA ELABORACIÓN:**
DESCRIPCION DEL PROYECTO	
OBJETIVOS ESTRATEGICOS	
OBJETIVOS DEL PROYECTO	
General	
Específicos	
JUSTIFICACIÓN DEL PROYECTO	

PRODUCTOS Y/O ENTREGABLES		
SUPUESTOS		
RESTRICCIONES		
DEPENDENCIAS		
RIESGOS DEL PROYECTO		
HITOS DEL PROYECTO		
Actividad	fecha estimada	Responsable
PRESUPUESTO ESTIMADO		
GERENTE PROYECTO, RESPOSABILIDADES Y NIVEL DE AUTORIDAD		
REQUERIMIENTOS DE APROBACION DEL PROYECTO		
RECURSOS PREASIGNADOS		
IDENTIFICACION DE INVOLUCRADOS		
Directos		
Indirectos		
FIRMAS		
PATROCINADOR	**GERENTE PROYECTO**	

Fuente: propia bajo las instrucciones de la guía del PMBOK

- Identificar los Interesados

Debemos identificar aquellas personas u organizaciones que los intereses pueden ser afectados de manera positiva o negativa, para lograr la captura pertinente, se planea el registro de los interesados con los siguientes cuadros:

Tabla 9 Registro de Interesados

	IDENTIFICACION				
ID	**Nombre Completo**	**EMPRESA**	**Cargo/Rol**	**Información Contacto**	**Clase**
1					
2					
3					
4					
5					

Fuente: propia bajo las instrucciones de la guía del PMBOK

Tabla 10 Registro de Clasificación

	CLASIFICACION							Prominencia	
ID	**Requerimientos**	**Expectativa**	**Poder**	**Interés**	**Influencia**	**Impacto**	**Conocimiento**	**Urgencia**	**Legitimidad**
1									
2									
3									
4									
5									

Fuente: propia bajo las instrucciones de la guía del PMBOK

	ADICIONALES					
ID	**Tipo de Interesado**	**Nivel Participacion**	**BRECHA**	**Acciones para**	**Interesado Clave**	**¿Por qué?**

				Cerrar la Bracha		
1						
2						
3						
4						
5						

Fuente: propia bajo las instrucciones de la guía del PMBOK

Además de identificar a los interesados del proyecto debemos evaluar el nivel, estrategia o trato de que aplicara según las siguientes métricas:

Tabla 11 Matriz Poder / Interés

Matriz de poder - Interés		PODER (nivel autoridad)	
		Bajo	Alto
INTERES (Preocupación o	Bajo	Estrategia de Esfuerzo mínimo (Monitorizar)	Estrategia de Mantener satisfechos
	Alto	Estrategia de Mantener informados	Estrategia de Actores clave. Gestionar de Cerca.

Fuente: guía del PMBOK

Tabla 12 Matriz Poder / Influencia

Matriz de poder - influencia	PODER (nivel autoridad)	
	Bajo	Alto

INFLUENCIA (Involucramiento	Bajo	Mantener Informados con Mínimo Esfuerzo	Mantenerlos Informados y Nunca Ignorarlos
	Alto	Trabajar con ellos	Trabajar por Él

Fuente propia: bajo las instrucciones de la guía del PMBOK

Tabla 13 Matriz de Influencia / Impacto.

Matriz de influencia - Impacto		IMPACTO (Capacidad Para Efecturar Cambios al Planeamiento o Ejecución del Proyecto)	
		Bajo	Alto
INFLUENCIA (Involucramiento	Bajo	Mantener Informados con Mínimo Esfuerzo	Mantenerlos Informados y Nunca Ignorarlos
	Alto	Trabajar con ellos	Trabajar por Él

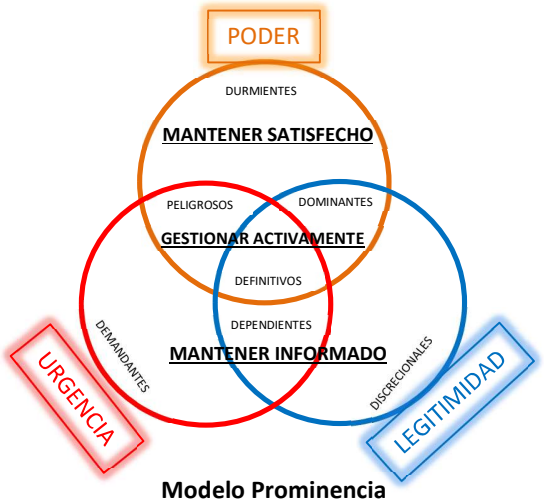
Fuente: bajo las instrucciones de la guía del PMBOK

Tabla 14 Matriz Poder / Dinamismo

Matriz de Poder - Dinamismo		PODER (nivel autoridad)	
		Bajo	Alto
DINAMISMO (Flexibilidad - Predictibilidad)	Bajo	Impredecible pero manejable	Los mayores Peligrosos u Oportunidades
	Alto	Pocos Problemas	Poderoso Pero Predecible

Fuente: bajo las instrucciones de la guía del PMBOK

Imagen 6 Modelo Prominencia



Modelo Prominencia

Fuente: bajo las instrucciones de la guía del PMBOK

1.8.2 Grupo Procesos de Planificación

- Plan Para la Dirección del proyecto

La pretensión de este apartado tiene gran importancia puesto que en esta sección definiremos la manera en que el proyecto se ejecuta, se monitorea, control y cierra. Para la realización de este plan es necesario tener en cuenta el acta del proyecto creado en el punto anterior siendo el punto de partida para establecer la planificación inicial del mismo. También debemos tomar con una entrada para la realización de este plan, las salidas de otros procesos. Se debe resaltar los factores ambientales de la empresa, por ejemplo: estándares o leyes gubernamentales, ares específicas y especializadas, otros sistemas de información, estructura y cultura organizacional, infraestructura, gestión de personal.

En Esta sesión plantearemos la forma clave mediante documento central que define la base para todo el trabajo del proyecto. Usaremos como entrada el acta de constitución, salida de otros procesos, factores ambientales, activos de los procesos de la organización. Este documento describe el modo en que el proyecto será ejecutado, monitoreado y controlado, integrando y consolidando los planes y líneas base secundarios de los procesos de planificación. Debemos tomar en cuenta las demás especificaciones que dictamina la guía del PMBOK que están por fuera de la presente descripción. Para favorecer el plan de la dirección del proyecto se plantea el siguiente esquema para futuro diligenciamiento:

Tabla 15 Plan Para la Dirección del Proyecto

Plan para la Dirección del Proyecto		
NOMBRE DEL PROYECTO		**IDENTIFICADOR**
		Nro. Actualización

REQUISITOS DEL PROYECTO
REQUISITOS DEL PRODUCTO

Definición del Proyecto	

Línea Base del Alcance	
Enunciado del Alcance	
Descripción del alcance	
Entregables Principales	
Supuestos	
Restricciones del proyecto	

Línea Base del Cronograma

Línea Base del Costo

Planes necesarios para la realización del proyecto	
Plan	**Descripción**
Plan de gestión del alcance	
Plan de gestión de los requisitos	
Plan de gestión del cronograma	
Plan de gestión de los costos	
Plan de gestión de la calidad	
Plan de mejoras del proceso	
Plan de gestión de los recursos humanos	
Plan de gestión de las comunicaciones	
Plan de gestión de los riesgos	

Plan de gestión de las adquisiciones	
Plan de gestión de los interesados	

Fuente: propia bajo las instrucciones de la guía del PMBOK

- Planificar la Gestión del Alcance.

Este proceso permitirá gestionar el alcance del proyecto que definirá y controlará qué y que no se incluye en el proyecto.

Se plantea la siguiente propuesta para registrar el alcance del proyecto a desarrollar según se estipule en el acta de inicio y ECT.

Tabla 16 Definición alcance del proyecto

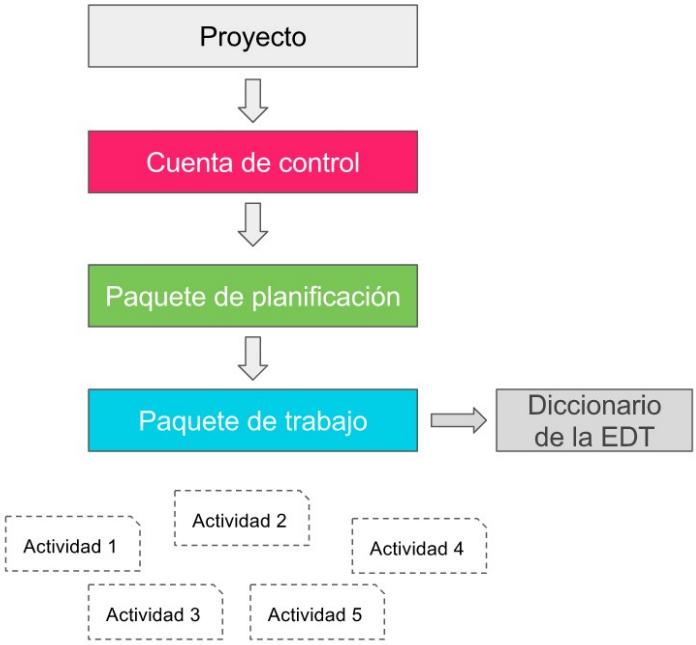
Alcance 1:			
ID Entregable: 01			
Id Sub-Entregable	Sub-Entregable	Descripción	Criterio o Requisito de Aceptación
ID Entregable: 02			
Descripción		Criterio de aceptación	
ID Entregable: 03			
Descripción		Criterio de aceptación	
ID Entregable: 04			
Descripción		Criterio de aceptación	
ID Entregable: 05			
Descripción		Criterio de aceptación	

Fuente: propia bajo las instrucciones de la guía del PMBOK

- Crear la EDT / WBS

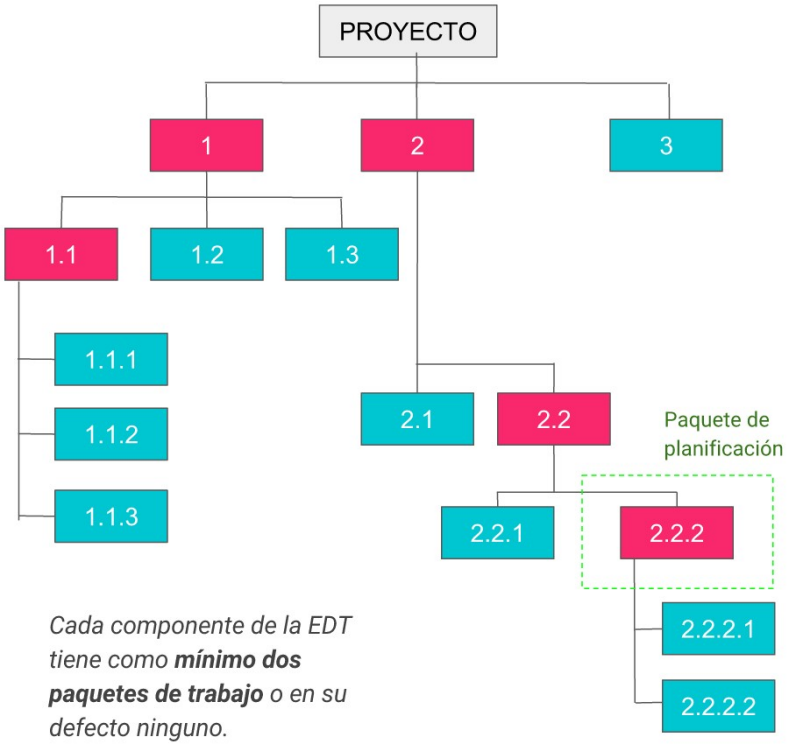
Para ello utilizaremos el software libre WBS Chart Pro que nos permitirá la creación y definición de la estructura detalla de trabajo con los entregables.

Imagen 7 Estructura EDT



Fuente: propia bajo las instrucciones de la guía del PMBOK

Imagen 8 Ejemplo EDT



Fuente: bajo las instrucciones de la guía del PMBOK

1.9 FASE 3. ALCANCE DEL PROYECTO SEGÚN LA GUÍA PMBOK.

El alcance del proyecto será definido mediante la guía del PMBOK siendo primordial la revisión minuciosa de los grupos de proceso de Inicio y planificación, dado los tiempos para la entrega del proyecto también limitaremos los procesos contenidos en el grupo de planificación.

El alcance del proyecto según la guía del PMBOK será definido en la Proceso "Planificar la Gestión del Alcance". En la definición del alcance se relacionará los entregables según como este estipulado en la creación del EDT.

El alcance para el proceso de Inicio contemplados en el PMBOK se estipula el acta de constitución y el registro de los interesados. Con respecto al proceso de planificación se

contemplan la revisión de los procesos de: Desarrollar el plan para la dirección de proyecto, Planificar la Gestión del Alcance, Recopilar Requisitos, Definir el Alcance, Crear la ETD/WBS, Planificar la gestión del Cronograma, Definir las actividades, Secuenciar las Actividades, Estimar los recursos de las actividades, estimar la duración de las actividades y desarrollar el cronograma.

1.10 FASE 4. PLANES DE GESTIÓN CONTEMPLADOS EN EL ALCANCE.

Dado el alcance del proyecto, se contempla que se realizarían la gestión de la integración donde se incluyen los procesos y actividades necesarias para identificar, definir, combinar, unificar y coordinar los diversos procesos y actividades de la dirección del proyecto.

Con respecto a la gestión del alcance del proyecto relacionada en el PMBOK, nos permitirá garantizar que el proyecto incluya todo el trabajo requerido y únicamente el trabajo para completar el proyecto con éxito de tal forma que se logre enfocar en definir y controlar que se incluye y que no se incluye en el proyecto.

Para el alcance relacionado en la fase 3 con respecto a la “Gestión del tiempo del proyecto”, se incluyen los procesos requeridos y alcanzables para gestionar la terminación.

Desarrollo.

1.11 SITUACIÓN ACTUAL.

Pertenecer a la institución implica conocer de cerca la situación y estado actual con respecto a los logros alcanzados para llegar a proteger la información importante como lo es las historias clínicas principalmente y registros asociados como su respectiva facturación y desde luego el estado financiero de la misma. Dada la experiencia y contacto con el personal de redes y tecnología, tenemos información que la institución cuenta con un dispositivo de red llamado Servidor SonicWall que protege en general la red mediante su Firewall incorporado, el administrador configuro algunas políticas para restringir el uso de internet como de redes sociales y páginas no autorizadas. En la entrevista con el personal encargado de las redes, se nos informa que esta información no le tiene respaldo ni documentada, en cuyo caso se da la oportunidad y recomendación dada la prioridad, de que se realice dicha actividad este servidor.

Con respecto a la configuración del servidor de Base de Datos, el departamento de sistemas posee clave de acceso y limitada a ciertas acciones de insertar, eliminar, actualizar, como también realizar cambios en Store Procedure. En este aspecto es notables que existen los controles necesarios y relativos al perfil del usuario que requiere la utilización de la base de datos. De igual forma con el servidor de aplicación de producción donde el administrador local del sistema no posee permisos de ningún tipo. En una oportunidad se tuvo contacto con el DBA para indagar sobre la documentación pertinente de estas políticas, pero no se obtuvo respuesta, aunque dada la configuración evidente existe el supuesto control y seguridad pertinentes para tener acceso y manejo de los servidores.

Existen algunos documentos que han sido generados acorde a las necesidades por el cumplimiento de alguna norma o exigencia técnica en los requisitos de alguna superintendencia, con información de políticas de calidad, protección de datos, seguridad, pero se considera que deben ser evaluadas nuevamente para verificar si se encuentra alineada a la filosofía institucional y se acoplan a la misma.

En términos generales, la fase 1 del capítulo anterior, nos muestra un avance poco significativo con respecto a los dominios implementados de la NTC/ISO 27002. Esto implica que el esfuerzo es mayor para lograr planificar todo el esquema que comprende la NTC/ISO 27001:2013.

1.12 ACTA DE CONSTITUCIÓN SEGÚN LA GUÍA PMBOK

La planificación del proyecto inicia con el Acta de Constitución y su finalidad es poder iniciar formalmente con la aprobación del proyecto, asignar un director de proyecto y su autoridad. Debemos tener presente que esta acta no es un contrato, pues no existen consideraciones, compromisos o intercambios monetarios en el ejercicio, netamente es para apoyar la planificación del proyecto siendo la base fundamental del PMBOK.

Podemos seguir el siguiente esquema acta registrada:

Tabla 17 Acta constitución

ACTA CONSTITUCION	
NOMBRE DEL PROYECTO	**IDENTIFICADOR**
PLAN PARA EL DISEÑO DEL SISTEM DE GESTION DE SEGURIDAD DE LA INFORMACION NTC/ISO 27001:2013 EN LA CLINICA MEDICAL DUARTE.	PMO-1001
JEFE PROYECTO	**FECHA ELABORACIÓN:**
VICTOR MANUEL GARNICA	01/01/2019
DESCRIPCION DEL PROYECTO	
El proyecto diseñara paso a paso la ruta a seguir para lograr la implementación del SGSI según la norma técnica colombiana ISO 27001:2013. Para la realización de este proyecto, es necesario recopilar información acerca del estado que maneja la institución, recopilar información sobre la familia NTC ISO 27000	
OBJETIVOS ESTRATEGICOS	
• Verificar y resaltar la importancia de la familia ISO 27000 • Formar un grupo de trabajo para el estudio detallado de la NTC ISO 27001:2013 • Contextualizar la NTC ISO 27001:2013 • Revisar y estudiar las referencias que plasma la NTC ISO 27001:2013 para el estudio particular.	

- Revisar, estudiar y contextualizar los objetivos de control y controles de referencia de la ISO 27002:2013
- Creación de mapas conceptuales.
- Recopilar todas las referencias normativas y estudiarlas.
- Estudio y contextualización de la norma técnica colombiana ISO 31000 para la gestión del riesgo.

OBJETIVOS DEL PROYECTO

General

- Estructurar planes de gestión para planificar la implementación del SGSI.
- Elaborar los documentos con los planes de gestión.
- Elaborar los documentos con los requisitos y reglamentarios de la NTC – ISO 27001:2013.

Específicos

- Contextualizar la organización.
- Definir el liderazgo y compromisos.
- Definir la política de la seguridad de la información.
- Definir roles, responsabilidades y autoridades.
- Documentar los riesgos.
- Valoración del riesgo.
- Tratamiento de los riesgos.
- Controlar los riesgos.
- Formular un plan de tratamiento de los riesgos.
- Determinar los recursos del SGSI
- Establecer canales y flujo de la comunicación.
- Establecer mecanismos para el control de la información.
- Establecer mecanismos para la planificación y control operacional del SGSI.
- Evaluar el desempeño del SGSI.
- Crear y documentar las mejoras continuas.

JUSTIFICACIÓN DEL PROYECTO

La razón de este proyecto, reside en la oportunidad de poner en práctica los cursos aprendidos durante la especialización de seguridad informática, en conjunto con el apoyo otorgado por la gerencia de la clínica medical duarte y tener la oportunidad de planificar el Sistema de Gestión de la Seguridad Informática como una decisión estratégica para establecer, implementar, mantener y aplicar mejoras continuas en dicho sistema de tal forma que aumentara y promulgara el estado actual para preservar la confidencialidad integridad y disponibilidad de la información.

PRODUCTOS Y/O ENTREGABLES

Documento con la normativa, análisis y construcción del SGSI para la institución.

SUPUESTOS

- Compromiso de la alta dirección
- Compromisos de las áreas involucradas.

- Contextualizar la norma ISO 27001 para la fácil traducción y entendimiento del mismo.

RESTRICCIONES

Presupuesto por definir
Fecha de entrega para inicio del 2021.

DEPENDENCIAS

-

RIESGOS DEL PROYECTO

- Tiempo y presupuesto errados
- Conflictos laborales
- Abandono de los interesados directos.
- Abandono temporal del equipo de trabajo.
- Plazo de hitos con mucho optimismo
- Roles y responsabilidades mal definidas.
- Comunicación inconclusa o escasa
- Errada interpretación de los objetivos.
- Cambios imprevistos, tema que esta subsanado.
- Falta patrocinador
- Baja la retroalimentación entre equipo de trabajo y empresa.
- Requisitos mal interpretados.
- Nuevos requerimientos fuera del plazo
- Cambios en la norma.
- Falta de presupuesto.
- Problemas en la capacitación del personal

HITOS DEL PROYECTO

Actividad	fecha estimada	responsable
Acta constitución del proyecto	Semana 1	
Identificación de los interesados	Semana 2	
Estructura de Desglose de Trabajo.	Semana 3	
Documentación planificación para el SGSI	Semana 10	
Documentos plan de gestión entregable	Semana 20	

PRESUPUESTO ESTIMADO

212.700.000

GERENTE PROYECTO, RESPOSABILIDADES Y NIVEL DE AUTORIDAD

Victor Garnica

Ejecutar, diseñar, evaluar, controlar y aplicar mejora continua

REQUERIMIENTOS DE APROBACION DEL PROYECTO

Documento SGSI

RECURSOS PREASIGNADOS

IDENTIFICACION DE INVOLUCRADOS	
Directos	
• Alta gerencia • Directivos • Coordinadores • Auxiliares	
Indirectos	
• Auditores externos • Proveedores	
FIRMAS	
PATROCINADOR	**GERENTE PROYECTO**

Fuente: propia bajo las instrucciones de la guía del PMBO

1.13 INTERESADOS

Es parte fundamental en la planificación, registrar los interesados del proyecto para ello se propone el diligenciamiento del siguiente esquema:

Tabla 18 Identificación interesados

	IDENTIFICACION				
ID	**Nombre Completo**	**EMPRESA**	**Cargo/Rol**	**Información Contacto**	**Clase**
1	Javier Duarte	CMD	Alta Gerencia	privada	Interno
2	Victor Garnica	CMD	Director Proyecto	privada	Interno
3	Analista	CMD	Auxiliar Control	privada	Interno
4	Auditor	CMD	Auditor	-	externo
5	Directivos	Grupo Holding	Junta Directiva	-	Interno

Fuente: propia bajo las instrucciones de la guía del PMBOK

Tabla 19 Clasificación Requerimientos

	CLASIFICACION							Prominencia	
ID	Requerimientos	Expectativa	Poder	Interés	Influencia	Impacto	Conocimiento	Urgencia	Legitimidad
1	Presentación del proyecto	A	A	A	A	A			
2	Elaboración del proyecto	A	A	B	B	B			
3	Estudio del proyecto	B	B	B	B	B			
4	Estudiar y auditar	B	B	A	B	B			
5	Presentación del proyecto	B	A	B	B	B			

Fuente: propia bajo las instrucciones de la guía del PMBOK

Tabla 20 **Tipo de interesados**

	ADICIONALES					
ID	**Tipo de Interesado**	**Nivel Participación**	**BRECHA**	**Acciones para Cerrar la Bracha**	**Interesado Clave**	**¿Por qué?**
1	Latente - Demandante	A			SI	
2	Latente - Demandante	A			SI	
3	Latente - Discrecional	A			NO	
4	Expectante - Dominante	B			NO	
5	Expectante - Peligroso	B			NO	

Fuente: propia bajo las instrucciones de la guía del PMBOK

1.14 PLAN DE DIRECCIÓN DEL PROYECTO

Tabla 21 **Plan dirección de proyecto**

Plan para la Dirección del Proyecto		
NOMBRE DEL PROYECTO	PLAN PARA EL DISEÑO DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION NTC/ISO 27001:2013 EN LA CLINICA MEDICAL DUARTE.	**IDENTIFICADOR**
		PMO-1002
		Nro. Actualización
		1

REQUISITOS DEL PROYECTO
• Recursos asignados. • Personal capacitado. • Estudio y Conocimiento de la norma. • Interpretación de la norma. • Auditor externo en calidad. • Búsqueda y visita de referentes con acreditación SGSI.
REQUISITOS DEL PRODUCTO
• Cumpla con los requisitos de la norma NTC-ISO 27001:2013 • Documento estructurado según las normas internas de la institución.

Definición del Proyecto	

Línea Base del Alcance	
Enunciado del Alcance	
Descripción del alcance	Aplicado para la institución descrita en la fase 1.
Entregables Principales	Documentos con la estructuración de la NTC-ISO 27001:2013 alineados con el SGC de la institución.
Supuestos	Compromiso de la alta gerencia para con el plan estratégico en la alineación de la norma
Restricciones del proyecto	Fecha entrega estimada

Línea Base del Cronograma
Este cronograma estará basado en el aprendizaje inicial y capacitación a los colaboradores que se integren al proyecto, para ello se establece de un mes de capacitación, además para la planificación de los planes de PMBOK necesarios para llevar a cabo este proyecto con un máximo de 6 meses. Se estima que para la implementación se tomen entre 2 y 3 años.

Línea Base del Costo
El costo base por definir según el alcance, cronograma del proyecto, requisitos.

Planes necesarios para la realización del proyecto	
Plan	**Descripción**
Plan de gestión del alcance	Se define el alcance del proyecto donde de establecer el proceso para crear la EDT, como se mantendrá y aprobará el mismo, como se hará la entrega formal y la solicitud de los cambios al proyecto
Plan de gestión de los requisitos	Se definirá la planificación, monitorización y entrega de reportes sobre las actividades y que se debe informar. Además, cambios del producto, analizar el impacto, monitoreo, seguimiento.
Plan de gestión del cronograma	Estableceremos los criterios para mantener el cronograma para que las actividades se lleven a cabo.

Fuente: propia bajo las instrucciones de la guía del PMBOK

Para continuar con el proceso y cumplimiento de la guía PMBOK, se sugiere la utilización del siguiente formato para complementar el plan de dirección de proyecto.

Tabla 22 **Plan de gestión del alcance de proyecto**

Plan de Gestión del Alcance de Proyecto (PGAP)		
NOMBRE DEL PROYECTO	PLAN PARA EL DISEÑO DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION NTC/ISO 27001:2013 EN LA CLINICA MEDICAL DUARTE.	**IDENTIFICADOR**
		PMO-1003
		Nro. Actualización
		1

PROPOSITOS DEL PGAP
Cómo será definido, desarrollado, monitoreado, controlado y verificado el alcance.

DESARROLLO DEL ENUNCIADO DEL ALCANCE DEL PROYECTO
El alcance será canalizado mediante el estudio de las normas propuestas en el proyecto, relacionado con la norma NTC/ISO 27001

ESTRUCTURA DE LA EDT/ WBS
Se hará uso de la herramienta online wbstool.com para la construcción de la estructura detallada de trabajo.

DICCIONARIO DE LA EDT / WBS
Se debe registrar cada actividad registrada en la EDT en el formato propuesto.

CAMBIOS DEL ALCANCE
Se recomienda no realizar cambios al alcance de este proyecto para no causar traumas como tampoco extender el cronograma o tiempo de ejecución de este. Sin embargo, de existir cambios, serán socializados en las reuniones de avances del proyecto, informando el estado de estos cambios y la magnitud del cambio que le producirá al proyecto

ACEPTACION DE LOS ENTREGABLES
Según estudio del cronograma y validación de requisitos. Es pertinente contar con la opinión o juicio de un experto que nos permita tener la certeza y confianza sobre los entregables para que cumplan con los objetivos de los entregables

INTEGRACION DE LOS REQUISITOS Y EL ALCANCE
Según el impacto del requisito, con relación a la line base del proyecto, serán aprobados por el director del proyecto bajo previo estudio de factibilidad.

Fuente: propia bajo las instrucciones de la guía del PMBOK

Tabla 23 Plan de gestión de los requisitos del proyecto

Plan de Gestión de Los Requisitos del Proyecto (PGRP)		
NOMBRE DEL PROYECTO	PLAN PARA EL DISEÑO DEL SISTEM DE GESTION DE SEGURIDAD DE LA INFORMACION NTC/ISO 27001:2013 EN LA CLINICA MEDICAL DUARTE.	**IDENTIFICADOR**
		PMO-1004
		Nro. Actualización
		1

PROPOSITOS DEL PGRP
Permitirá analizar, documentar y gestionar los requisitos del proyecto.

ACOPIO DE LOS REQUISITOS
• Lectura y captura de mapa mental de la norma seleccionada. • Investigación de campo y recopilación de información. • Búsqueda de antecedentes de instituciones certificadas bajo la norma seleccionada. • Entrevistas con usuarios y personal externo.

CLASIFICACION DE LOS REQUISITOS
Se recopilarán lo requisitos y se enmarcarán los siguientes grupos: Requisitos de Negocio: estarán acorde con la institución ya que se desea alcanzar la acreditación en salud mediante la ejecución y documentos de la entrega. Requisitos de Interesados: deberá satisfacer a los interesados del proyecto. Tomar en cuenta que también se deben tener en cuenta los interesados externos, ya que pueden ser parte directa o indirecta con potencial beneficios. Requisitos de las Soluciones: las soluciones deben abarcar la parte tecnológica y sus requerimientos, que permitan mejorar los procesos que se requieren para la norma seleccionada en el proyecto. Se debe verificar que requisitos de capacitación y a quien va dirigido. Requisitos Temporales: estos no deben tener mayor influencia en el proyecto

PRIORIZACION DE LOS REQUISITOS
Con el estudio minucioso de las normas, se determinará la priorización. Se clasificarán todos los requisitos y se asignara una escala de 1 a 10 para considerar el impacto y el poder que posee sobre el proyecto.

TRAZABILIDAD DE LOS REQUISITOS

Haremos uso de la matriz de trazabilidad que propone la guía PMBOK. Esto nos permitirá mantener un estado de los requisitos.

GESTION DE LA CONFIGURACIÓN
Los cambios pueden ser solicitados por cualquier miembro del equipo. Esta solicitud será enviada al gerente del proyecto, quien analizará si la solicitud afecta y que grado puede afectar los requisitos y el cronograma del proyecto. Determinará si se acepta el cambio o por lo contrario lo rechaza, con la observación de abordar dicho cabio en fases futuras de actualización del proyecto.

Fuente: propia bajo las instrucciones de la guía del PMBOK

Tabla 24 Matriz Trazabilidad de Requisitos

Matriz de Trazabilidad de Requisitos		
NOMBRE DEL PROYECTO	PLAN PARA EL DISEÑO DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION NTC/ISO 27001:2013 EN LA CLINICA MEDICAL DUARTE.	**IDENTIFICADOR**
		PMO-1006
		Nro. Actualización
		1

ID	Id.Aso	Descripción Requisito	entregable ETD	Estado

Fuente: guía del PMBOK

Tabla 25 Plan de gestión del cronograma del proyecto

Plan de Gestión del Cronograma del Proyecto (PGCP)		
NOMBRE DEL PROYECTO	PLAN PARA EL DISEÑO DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION NTC/ISO 27001:2013 EN LA CLINICA MEDICAL DUARTE.	**IDENTIFICADOR**
		PMO-1005
		Nro. Actualización
		1

PROPOSITO DE PGCP
Mediante la utilización de métodos que permitan calcular el tiempo que tomara la gestión del proyecto

METODOLOGIA PARA LA GESTION DEL CRONOGRAMA
Método del Camino Critico (CPM) y Cadena Crítica (CCM).

HERRAMIENTAS PARA PGCP
Microsoft Proyect o diseño de cada método sobre un procesador de cálculos.

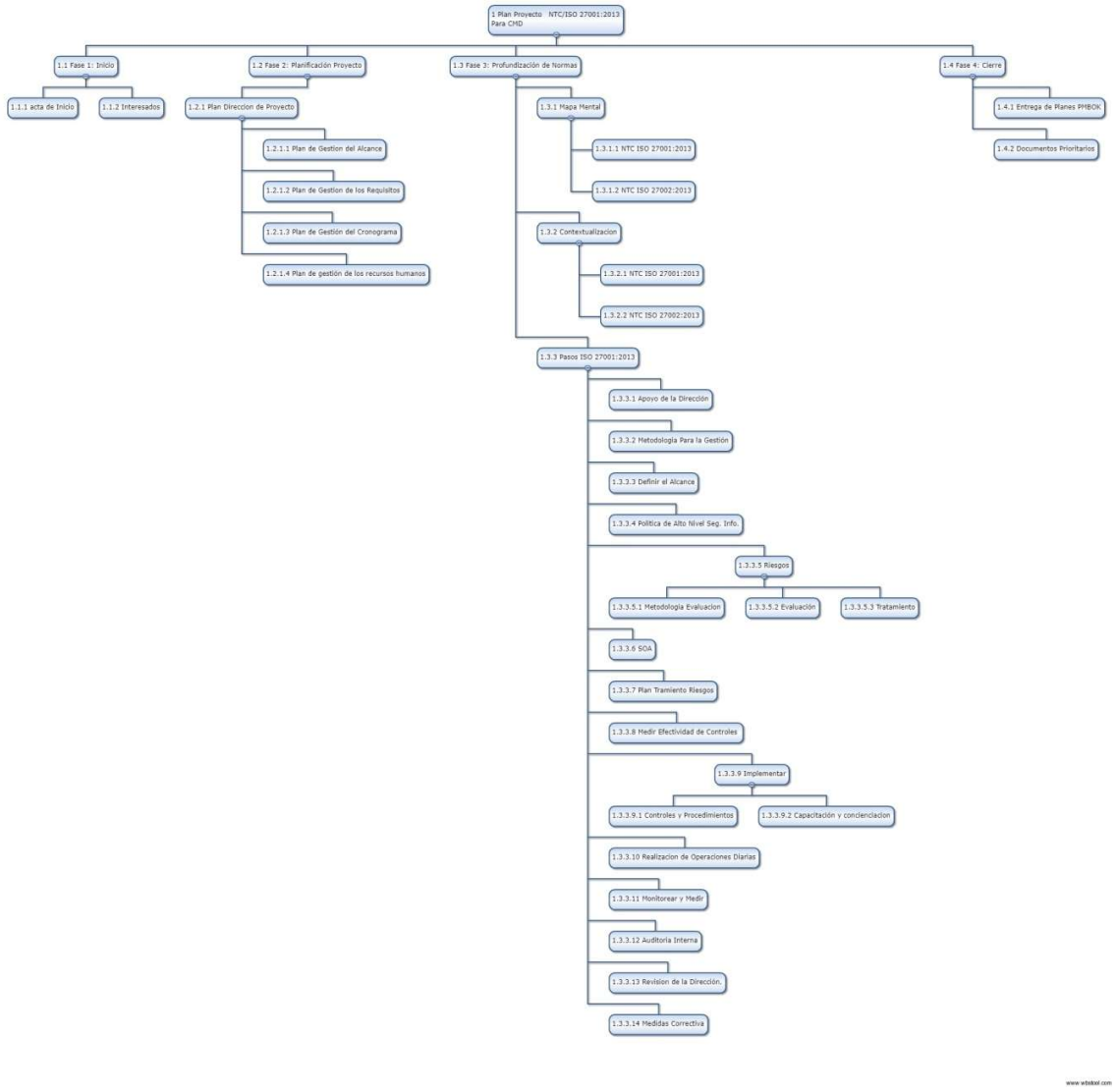
REPORTE Y FORMATO DEL CRONOGRAMA

PROCESO DE GESTION DEL CRONOGRAMA	
identificación de las actividades	Estas son registradas en la Estructura Detallada de Trabajo (EDT), mediante el estudio detallado de los objetivos registrados en el acta del proyecto
secuenciación de las actividades	Se dará inicio según niveles registrados en el EDT. Se definirá cuando inicia una actividad si esta depende de otra. Se hará uso de los diagramas PERT para establecer relaciones
estimación de los recursos	Entre los recursos a ser necesarios se debe contar con el juicio de un experto en todas las áreas posibles en especial las detalladas en el acta del proyecto. Desde luego entre estos recursos se debe contar con un software para la gestión del proyecto.
estimación de esfuerzos y duración	Es importante en todos los aspectos cruciales del proyecto, contar con un juicio de un ente externo y experto para que nos permita dar mejor orientación y punto de vista de los temas. En este punto se requiere conocer sobre la estimación de tiempos y como calcular. También debemos contar con previo conocimiento sobre duración por analogía y por parámetros.
actualización, monitoreo y control	Debemos usar una metodología que nos permitirá controlar y brindar seguimiento a las actividades. Se propone realizar una sesión de trabajo que permita conocer y profundizar más sobre metodologías como: valor ganado o control de margen en cadena critica.

Fuente: propia bajo las instrucciones de la guía del PMBOK

1.15 EDT / WBS

La siguiente grafica muestra la estructura de desglose de trabajo para nuestro proyecto en la cual se plantea en 4 fases, siendo la más amplia la Fase III para estudiar y profundizar.



1.16 DICCIONARIO EDT – WBS

Basado en la EDT anterior, debemos hacer uso del siguiente esquema para definir los componentes del gráfico.

Tabla 26 Diccionario EDT/WBS 1.3.1

DICCIONARIO EDT WBS			
NOMBRE DEL PROYECTO	PLAN PARA EL DISEÑO DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION NTC/ISO 27001:2013 EN LA CLINICA MEDICAL DUARTE.	**IDENTIFICADOR**	PMO-1006
		Nro. Actualización	1
ID ENTREGABLE	1.3.1	**NOMBRE ENTREGABLE**	Mapa Mental

DESCRIPCION ENTREGABLE
Se realizará un estudio detallado de la norma que permita contextualizar, comprender y entender de forma gráfica las ideas representativas de cada norma, de tal forma que el grupo de trabajo pueda entender en un lenguaje sencillo la misma

DURACION	3D	**FECHA INICIO**	Por Definir	**FECHA FINAL**	Por Definir

HITOS	FECHA
Grafica Mapa Mental	2020

REQUISITOS DE CALIDAD
• El uso de imágenes, símbolos, códigos y dimensiones a lo largo de su mapa mental. • Seleccionar palabras clave y de impresión utilizando letras mayúsculas o minúsculas. • Cada palabra/imagen es mejor solo y sentado en su propia línea. • Las líneas deben estar conectadas, a partir de la imagen central. Las líneas se vuelven más delgadas a medida que irradian hacia fuera desde el centro. • Hacer que las líneas sean de la misma longitud que la palabra/imagen de apoyo. • El uso de múltiples colores en todo el mapa mental, para la estimulación visual y también para la codificación o la agrupación. • Desarrollar su propio estilo de los mapas mentales. • El uso de énfasis y mostrar las asociaciones/enlaces en su mapa mental.

• Mantener el mapa mental claro y ordenado mediante el uso radial de jerarquía o contornos para abrazar sus ramas.

CRITERIOS DE ACEPTACION
Cumpla con las pautas establecidas

REFERENCIAS TECNICAS
Archivo JPG o PNG, utilización de herramientas como FreeMind o paginas online.

CONSIDERACIONES CONTRACTUALES
Ninguna

INFORME DE RIESGOS
• Estructurar un mapa más complejo que la misma norma.

COSTO ESTIMADO							
Recurso	**Mano de obra**			**Materiales**			**TOTAL COSTO**
	Hora / Días	*Tarifa*	*Total*	*Hora*	*Tarifa*	*Total*	
Software Libre	3D	0		3D			$ 0

Fuente: propia bajo las instrucciones de la guía del PMBOK

Tabla 27 **Diccionario EDT/WBS 1.3.2**

DICCIONARIO EDT WBS			
NOMBRE DEL PROYECTO	PLAN PARA EL DISEÑO DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION NTC/ISO 27001:2013 EN LA CLINICA MEDICAL DUARTE.		**IDENTIFICADOR**
			PMO-1006
			Nro. Actualización
			1
ID ENTREGABLE	1.3.2	**NOMBRE ENTREGABLE**	Contextualización

DESCRIPCION ENTREGABLE
Basado en el mapa mental de la ETD anterior y las notas recopiladas en el estudio inicial de las normas, se pretende poner en contexto y ayudas técnicas de cada punto estudiado de tal forma que se logre entender con más facilidad los requerimientos.

DURACION	14D	FECHA INICIO	Por Definir	FECHA FINAL	Por Definir

HITOS	FECHA
Documento clave con el contexto de las normas a estudiar.	2020

REQUISITOS DE CALIDAD
• Debe tener relación, coherente e interpretación de la normas consultadas.

CRITERIOS DE ACEPTACION
Texto Interpretado.

REFERENCIAS TECNICAS
Toda la familia ISO 27000 2013

CONSIDERACIONES CONTRACTUALES
Ninguna

INFORME DE RIESGOS
• Estructurar un mapa más complejo que la misma norma.

COSTO ESTIMADO							
Recurso	Mano de obra			Materiales			TOTAL COSTO
	Hora / Días	*Tarifa*	*Total*	*Hora*	*Tarifa*	*Total*	
Software Libre	3D	0		3D			$ 0

Fuente: propia bajo las instrucciones de la guía del PMBOK

Tabla 28 Diccionario EDT/WBS 1.3.3.1

DICCIONARIO EDT WBS		
NOMBRE DEL PROYECTO	PLAN PARA EL DISEÑO DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION NTC/ISO 27001:2013 EN LA CLINICA MEDICAL DUARTE.	IDENTIFICADOR
		PMO-1006
		Nro. Actualización
		1

ID ENTREGABLE	1.3.3.1	NOMBRE ENTREGABLE	Apoyo de la Dirección

DESCRIPCION ENTREGABLE
El compromiso de la dirección general, juega un papel importante para la aceptación y ejecución del proyecto como también para la asignación de recursos.

DURACION	7D	FECHA INICIO	Por Definir	FECHA FINAL	Por Definir

HITOS	FECHA
Documento acta de compromiso o acta del proyecto.	2020

REQUISITOS DE CALIDAD
• Apoyo de la dirección general

CRITERIOS DE ACEPTACION
Muestra sobre las ventajas para la aceptación y apoyo del proyecto.

REFERENCIAS TECNICAS
Archivo DOC.

CONSIDERACIONES CONTRACTUALES
Ninguna

INFORME DE RIESGOS
• Estructurar un mapa más complejo que la misma norma.

COSTO ESTIMADO							
Recurso	Mano de obra			Materiales			TOTAL COSTO
	Hora / Días	*Tarifa*	*Total*	*Hora*	*Tarifa*	*Total*	
Software Libre	3D	0		3D			$ 0

Fuente: propia bajo las instrucciones de la guía del PMBOK

Tabla 29 Diccionario EDT/WBS 1.3.3.2

DICCIONARIO EDT WBS			
NOMBRE DEL PROYECTO	PLAN PARA EL DISEÑO DEL SISTEMA DE GESTION DE SEGURIDAD DE LA	IDENTIFICADOR	PMO-1006

	INFORMACION NTC/ISO 27001:2013 EN LA CLINICA MEDICAL DUARTE.		Nro. Actualización
			1
ID ENTREGABLE	1.3.3.2	**NOMBRE ENTREGABLE**	Metodologías para la Gestión

DESCRIPCION ENTREGABLE
La utilización de una metodología para gestionar el proyecto esta planteado mediante la guía del Pmbok como parte de control y gestión para la planificación del proyecto. La Metodología Magerit también se estudiará para el análisis y gestión de riesgos. Estaba inmersa en la elaboración del mapa mental.

DURACION	7D	**FECHA INICIO**	Por Definir	**FECHA FINAL**	Por Definir

HITOS	**FECHA**
Descripción acta del proyecto	2020
Descripción Metodologías seleccionadas.	2020

REQUISITOS DE CALIDAD
• Este relacionado con el proyecto de SGI.

CRITERIOS DE ACEPTACION
Cumpla con las pautas establecidas

REFERENCIAS TECNICAS
Archivo JPG o PNG, utilización de herramientas.

CONSIDERACIONES CONTRACTUALES
Ninguna

INFORME DE RIESGOS
• Dificultades en traducir las metodologías de otros lenguajes. • Metodologías extensas y complejas de comprender.

COSTO ESTIMADO

Recurso	**Mano de obra**			**Materiales**			**TOTAL COSTO**
	Hora / Días	*Tarifa*	*Total*	*Hora*	*Tarifa*	*Total*	
Documento Metodología		0		3D			$ 0

Fuente: propia bajo las instrucciones de la guía del PMBOK

Tabla 30 Diccionario EDT/WBS 1.3.3.3

DICCIONARIO EDT WBS					
NOMBRE DEL PROYECTO	PLAN PARA EL DISEÑO DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION NTC/ISO 27001:2013 EN LA CLINICA MEDICAL DUARTE.			**IDENTIFICADOR**	PMO-1006
				Nro. Actualización	1
ID ENTREGABLE	1.3.3.3	**NOMBRE ENTREGABLE**	Definir el Alcance		

DESCRIPCION ENTREGABLE
Con el mapa mental, estudio de las normas podremos enmarcar un alcance y meta para lograr los objetivos.

DURACION	7D	**FECHA INICIO**	Por Definir	**FECHA FINAL**	Por Definir

HITOS	FECHA
Documento con la descripción del alcance del proyecto	2020

REQUISITOS DE CALIDAD
• Se encuentren alineados con la propuesta para lograr

CRITERIOS DE ACEPTACION
Desarrollo de los alcances sean medibles.

REFERENCIAS TECNICAS
Archivo JPG o PNG, utilización de herramientas.

CONSIDERACIONES CONTRACTUALES
Ninguna

INFORME DE RIESGOS
• No lograr el desarrollo final del alcance. • Descripción de alcances insuficiente.

COSTO ESTIMADO			
Recurso	**Mano de obra**	**Materiales**	**TOTAL COSTO**

	Hora / Días	*Tarifa*	*Total*	*Hora*	*Tarifa*	*Total*	
Documento Metodología		0		3D			$ 0

Fuente: propia bajo las instrucciones de la guía del PMBOK

Tabla 31 Diccionario EDT/WBS 1.3.3.4

DICCIONARIO EDT WBS				
NOMBRE DEL PROYECTO	PLAN PARA EL DISEÑO DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION NTC/ISO 27001:2013 EN LA CLINICA MEDICAL DUARTE.		**IDENTIFICADOR**	PMO-1006
			Nro. Actualización	1
ID ENTREGABLE	1.3.3.4	**NOMBRE ENTREGABLE**	Política Seguridad Informática	

DESCRIPCION ENTREGABLE
Redacción de una política de alto nivel sobre seguridad de la información.

DURACION	7D	**FECHA INICIO**	Por Definir	**FECHA FINAL**	Por Definir

HITOS	**FECHA**
Documento con la política de seguridad de la información.	2020

REQUISITOS DE CALIDAD
• Validación de la política se seguridad documentada. • Aprobación de la política de seguridad de la información.

CRITERIOS DE ACEPTACION
Políticas ajustadas a la institución.

REFERENCIAS TECNICAS
Archivo JPG o PNG, utilización de herramientas.

CONSIDERACIONES CONTRACTUALES
Ninguna

INFORME DE RIESGOS
• No lograr el desarrollo final del alcance.

• Descripción de alcances insuficiente.

COSTO ESTIMADO							
Recurso	**Mano de obra**			**Materiales**			**TOTAL COSTO**
	Hora / Días	*Tarifa*	*Total*	*Hora*	*Tarifa*	*Total*	
Documento Metodología		0		3D			$ 0

Fuente: propia bajo las instrucciones de la guía del PMBOK

Tabla 32 Diccionario EDT/WBS 1.3.3.5

DICCIONARIO EDT WBS			
NOMBRE DEL PROYECTO	PLAN PARA EL DISEÑO DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION NTC/ISO 27001:2013 EN LA CLINICA MEDICAL DUARTE.	**IDENTIFICADOR**	PMO-1006
		Nro. Actualización	1
ID ENTREGABLE	1.3.3.5	**NOMBRE ENTREGABLE**	Riesgos

DESCRIPCION ENTREGABLE
Se debe analizar minuciosamente los riesgos potenciales en los que pueda incurrir el proyecto, entre los cuales pueden ser riesgos técnicos, rendimiento, calidad. Etc.

DURACION	7D	**FECHA INICIO**	Por Definir	**FECHA FINAL**	Por Definir

HITOS	FECHA
Documento con los riesgos del proyecto. Riesgos generales, gerenciales, externos, organizacionales	2020

REQUISITOS DE CALIDAD
• Registro de riesgos al proyecto

CRITERIOS DE ACEPTACION
Riesgos aceptables que estén bajo vigilancia para que no se conviertan en un daño perjudicial para el proyecto

REFERENCIAS TECNICAS
Criterio de expertos, fuentes externas.

CONSIDERACIONES CONTRACTUALES
Ninguna

INFORME DE RIESGOS
• No lograr visualizar todos los potenciales riesgos desde el inicio del proyecto. • Riesgos convertidos en perjuicio para el proyecto. • Descontrol del proyecto para la toma de decisiones.

COSTO ESTIMADO							
Recurso	**Mano de obra**			**Materiales**			**TOTAL COSTO**
	Hora / Días	*Tarifa*	*Total*	*Hora*	*Tarifa*	*Total*	
Documento riesgos		0		7D			$ 0

Fuente: propia bajo las instrucciones de la guía del PMBOK

Tabla 33 Diccionario EDT/WBS 1.3.3.6

DICCIONARIO EDT WBS			
NOMBRE DEL PROYECTO	PLAN PARA EL DISEÑO DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION NTC/ISO 27001:2013 EN LA CLINICA MEDICAL DUARTE.	**IDENTIFICADOR**	PMO-1006
		Nro. Actualización	1
ID ENTREGABLE	1.3.3.6	**NOMBRE ENTREGABLE**	SOA

DESCRIPCION ENTREGABLE
Se redactará la declaración de aplicabilidad de tal forma que nos permitirá adicionalmente definir el alcance del sistema de gestión de seguridad de la información.

DURACION	7D	**FECHA INICIO**	Por Definir	**FECHA FINAL**	Por Definir

HITOS	FECHA
Documento SOA	2020

REQUISITOS DE CALIDAD
• Registro de riesgos al proyecto

CRITERIOS DE ACEPTACION
Objetivos de seguridad. Medidas de seguridad. Motivos de la implementación. Los elementos, objetivos y mecanismos implementados actualmente. Las exclusiones y justificación relacionado con el anexo A de la norma ISO 27001.

REFERENCIAS TECNICAS

CONSIDERACIONES CONTRACTUALES
Ninguna

INFORME DE RIESGOS
•

COSTO ESTIMADO

Recurso	Mano de obra			Materiales			TOTAL COSTO
	Hora / Días	*Tarifa*	*Total*	*Hora*	*Tarifa*	*Total*	
Documento riesgos		0		7D			$ 0

Fuente: propia bajo las instrucciones de la guía del PMBOK

Conclusiones

Poseer la información interna de la institución nos permitió conocer el estado actual de la institución con respecto a las actividades de seguridad de la información que maneja. Si bien son actividades dada la experiencia que poseen los administradores encargados, estos no tienen la seguridad de estar cumpliendo con normas estandarizadas como el Sistema de Gestión de Seguridad Informática. Siendo este unos de los objetivos iniciales del proyecto, es pertinente continuar revisando los cambios registrados en el Sistema de Gestión de Calidad que puedan surgir durante la ejecución del proyecto.

La administración de proyectos nos permitirá trazar los planes necesarios para estructurar un marco de trabajo que nos lleve a planificar con detalle cómo debemos realizar nuestro proyecto para la futura implementación de la norma NTC ISO 27001:2013, la pretensión de este documento es el direccionamiento estratégico que enmarque la utilización de la guía PMBOK como principal fuente para el control, trazabilidad, gestión y planificación en la deseada norma mencionada.

Par diagnosticar y analizar la situación actual de la institución, se hizo uso de entrevistas, inspección directa y conocer el trabajo realizado a la fecha tanto por el departamento de redes como de sistemas, nos permitió obtener un panorama actual de la institución con respecto al SGSI, observando que existen algunas actividades implementadas para proteger la institución y salvaguardar algunos activos, pero no logra alcanzar la mayoría de los controles especificados en la norma ISO 27001. La situación actual de la institución es ideal para poder planificar todas las putas de la norma, además tomar acciones y planes necesarios para su posterior ejecución.

Par definir el alcance del proyecto hemos trabajado con la ayuda de la guía PMBOK[18], donde nos brida las pautas para poder planificar y dar gestión al marco normativo propuesto. Se ha determinado y establecido la evaluación y revisión de los grupos de procesos de inicio y de planificación dados los tiempos que se tiene para el presente proyecto.

Se determinó y estableció entre los procesos de inicio y planificación la gestión de integración de proyecto y el alcance, como también la gestión de los interesados de este, para lograr ello se ha establecido los formatos y utilización de herramientas que sugiere la guía incorporar el acta de constitución, EDT. El estudio de los interesados del proyecto nos permitirá establecer una guía sobre los interesados y la influencia que puede tener en el proyecto y como tratar las necesidades y expectativas. Con esta estrategia daremos las pautas para prestar mayor atención en aquellos interesados que pueda beneficiar o afectar el proyecto.

Durante la estructuración en el plan de dirección de proyecto se establece los planes de gestión del proyecto que a su vez ayudaran a determinar el alcance del proyecto. Estos planes se establecieron en la sección pertinente para registrar la información correspondiente para determinar el Plan de gestión del alcance, de los requisitos, de gestión del cronograma.

El estudio de la norma NTC ISO 27001 2013, la norma ISO 27002 2013, la norma GTC-ISO 27003 2012, la norma GTC-ISO 27035 2012, la norma ISO-IEC 17799, la norma NTC-ISO 31000, la norma ISO-IEC 31010, son los documentos que se deben explorar y analizar con detenimiento para realizar un análisis completo para lograr complementar y alcanzar las certificaciones futuras.

[18] https://www.pmi.org/pmbok-guide-standards/foundational/pmbok

El éxito se encuentra en establecer, comprender cada norma, relacionarlas entre sí, seguir el programa planteado en la estructura de desglose de trabajo para interpretar cada norma y poder plantear las soluciones requeridas para el SGSI.

Recomendaciones

Se debe estructurar la EDT de tal forma que se traza y subdivida los entregables y el trabajo en componentes más pequeños para facilitar el manejo, que facilitara una visión estructurada de lo que se debe entregar. En lo posible se recomienda se incluya una segunda fase para complementar el presente trabajo a futuro incluyendo los grupos de proceso de ejecución, Grupos de proceso de Monitoreo y Control, finalmente el grupo de procesos de cierre.

Es Beneficioso completar y ampliar la gestión del proyecto con los fundamentos para la dirección de proyectos, donde se debe incluir la gestión para la integración del proyecto, gestión del tiempo, gestión del costo, gestión de la calidad, gestión de los recursos humanos, gestión de la comunicación, gestión de los riesgos, gestión de las adquisiciones (para la compra y adquisición de productos, servicios), gestión de los interesados (identificación de las personas, grupos u organizaciones).

Se recomienda el estudio de las normas descritas en el documento, esto le permitirá ampliar los conocimientos suficientes para poder documentar cada apartado de las normas relacionadas. Es recomendable hacer uso de las técnicas de planeación relacionadas en la guía del PMBOOK para poder llevar una planificación y organización en la construcción de los documentos requeridos en la norma.

Una auditoría interna es pertinente ejecutar periódicamente para analizar los avances y retroalimentar los puntos no conformes del proyecto. También es beneficioso realizar una auditoría externa por expertos en el SGSI, que nos darán su punto de vista para tener otro potencial enfoco de realizar y continuar con el plan estratégico para la gestión del proyecto y lograr la tan anhelada certificación en el SGSI.

La alta gerencia debe estipular y asignar recursos para realizar la adquisición del material necesario relacionado con las normas ISO ya que algunas no son de dominio público. Se debe investigar el costo de este y cuales normas son privadas. También se recomienda adicionar presupuesto para un grupo de trabajo de profesionales tanto en seguridad informática y auditores para el proyecto, ya que es fundamental asignar de forma independiente y exclusivos que solamente se dediquen al mismo para el beneficio de las partes involucradas.

Es fundamental conocer la norma ISO-27002:2013, para ello el documento que expresa los 14 dominios, 35 objetivos y 114 controles se deben tomar uno a uno, documentarlos con detalles según lo planeado mediante la estrategia del PMBOK para capturar en detalle las referencias básicas, junto a los recursos existentes tanto a nivel local, nacional e internacional. Esta búsqueda puede ser extensa, pero será gratificante para el proyecto en temas de conocimiento y recopilación de datos.

Bibliografía

C., B., & B., H. (2008). Project Management Pr (Vásquez & Rocío, 2013)actice. Generic or Contextual: A Reality Check. Project Management Journal.

Cuervo, S., (2010). Implementación ISO 27001 – empresa Ficticia. Recuperado de: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/64827/10/scuervoTFM0617presentaci%C3%B3n.pdf

Esan. (2016). Los cinco principios de COBIT 5. Recuperado de: https://www.esan.edu.pe/apuntes-empresariales/2016/06/los-cinco-principios-de-cobit-5/

Escuela Europea de Excelencia (2019). Que es y para qué sirve la declaración de aplicabilidad en ISO 27001. Recuperado de: https://www.escuelaeuropeaexcelencia.com/2019/08/que-es-y-para-que-sirve-la-declaracion-de-aplicabilidad-en-iso-27001/

Empresa chilena DNV-GL (2016) Que es y para qué sirve la norma ISO 27001. Recuperado de: https://www.esan.edu.pe/apuntes-empresariales/2016/05/que-es-y-para-que-sirve-la-norma-iso-27001/

Europen unión agency for cybersecurity. (2014) ISO / IEC – Estándar 13335 : 2014. Recuperado de: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/rm-ra-standards/iso-iec-standard-13335

ESET Security Report. ESET Security Report Latinoamérica (2017). Recuperado de: https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf

International Organization for Standardization. (s.f.). ISO/IEC 27000 family - Information security management systems. Recuperado el Junio de 2018, de ISO - International Organization for Standardization: https://www.iso.org/isoiec-27001-information-security.html

Isaca (2012) Marco de referencia Cobit 5. Recuperado de http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx

Iso (2013). Controles ISO 27002:2013 Recuperado de: http://iso27000.es/download/ControlesISO27002-2013.pdf

ISO / IEC 27034-1-2011 Information Technology, securit techniques – application security – parte 1. Recuperado de https://www.iso.org/standard/44378.html?browse=tc

ISO/IEC 27002:2013 (2013) El portal ISO 27002 en español. Recuperado de: http://iso27000.es/iso27002.html

Isotool Excellence (2015) ISO 17799 Recuperado De: https://www.pmg-ssi.com/2015/04/isoiec-17799-politica-de-seguridad/

Kosutic, D., (2013) ISO 27001/ ISO 22301 Base de Conocimientos. Lista de documentos obligatorios para la norma IS 27001. Recuperado de: https://advisera.com/27001academy/es/knowledgebase/lista-de-documentos-obligatorios-exigidos-por-la-norma-iso-27001-revision-2013/

León, A., (2014). Mapping COBIT 5 With IT Governance, risk an compliance at ecopetrol. Isaca recuperado de http://www.isaca.org/Knowledge-Center/cobit/cobit-focus/Pages/COBIT-Focus-Volume-3-July-2014.aspx#1

Marcos de referencia para la gestión de servicios de TI. Recuperado de: https://cobitweb.wordpress.com/2017/03/14/que-es-cobit/

Oré, A., (2014) Identificar y Priorizar "Stakerholders". https://es.slideshare.net/angeloremu/identificar-y-priorizar-stakeholders-sedipro-untels.

Portal De Soluciones Técnicas Y Organizativas A Los Controles De Iso/Iec 27002. Recuperado de: https://iso27002.wiki.zoho.com/ISO-27002.html

PMG-ISS SGSI (2014). Gestión de incidentes de seguridad de la información. Recuperado de https://www.pmg-ssi.com/2014/05/iso-27035-gestion-de-incidentes-de-seguridad-de-la-informacion/

PMI. (2013). Guía de los fundamentos para la dirección de proyectos (guía PMBOK®). Project Managed Institute. Quinta edición.

Recalde, V. & Alexandea, E. (2017). Elaboración del plan de gestión de seguridad de información en base a la metodología magerit para el Gobierno Autónomo Descentralizado Municipal de Antonio Ante (GADMAA). Recuperado de http://repositorio.utn.edu.ec/handle/123456789/7728

Saavedra, J., Alfoso, T., (2012). Modelo de gobierno de TI como apoyo al proceso de transformación digital en empresas de la industria editorial. Recuperado de: https://repository.icesi.edu.co/biblioteca_digital/bitstream/10906/70808/1/modelo_gobierno_procesos.pdf

Soto, D. (2016). ¿Qué es COBIT y para qué sirve? Recuperado de: https://nextech.pe/que-es-cobit-y-para-que-sirve/

Universidad EAFIT. (2007) Cobit, Modelo para auditoría y control de sistemas de información. Recuperado de: http://www.eafit.edu.co/escuelas/administracion/consultorio-contable/Documents/boletines/auditoria-control/b13.pdf

Vázquez, G., & Rocio, K. d. (2013) Aplicación de la metodología Magerit para el análisis y gestión de riesgos de la seguridad de la información aplicado a la empresa Pesquera e Industrial Bravito S.A. en la ciudad de Machala. Recuperado de http://dspace.ups.edu.ec/bitstream/123456789/5272/1/ups-ct002759.pdf

Vera, M. F., Molina, A.S., & Cedeño, M.L. (2017). Gobierno de las tecnologías de la información (TI) modelo COBIT 5.0. Recuperado de https://morebooks.de/store/es/book/gobierno-de-las-tecnologÃ-as-de-la-informaciÃ³n-ti-modelo-cobit-5-0/isbn/978-3-639-77848-9